Appendix C:
County of Los Angeles
Wireless LAN Guidelines

Wireless LAN Guidelines

Version 1.4

Reference: Countywide Master Information Security Policy

Developed by: Remote Access Work Group, Mitigation of Cyber Terrorism

1.0 PURPOSE

The purpose of this document is to establish guidelines for deploying and operating Wireless Local Area Networks (WLAN) in Los Angeles County government organizations. WLAN components are relatively inexpensive and the benefits they provide easily justify their deployment. This paper provides organization leaders with the practical understanding of the factors related to the deployment and the operation of WLAN. The products based on IEEE 802.11 standards that have been certified by Wireless Ethernet Compatibility Alliance (WECA) for Wi-Fi (wireless fidelity) compliance are dominant in the industry. The focus is on the Wi-Fi compliant technologies. There are other WLAN technologies using infrared or other frequency spectrums. Other products are usually proprietary or they have not gained wide acceptance in the industry, and are not addressed in these guidelines. However, the practices recommended in these guidelines may be used to mitigate risk associated with other wireless technologies.

1.0.1 RELEASE NOTES AND HISTORY LOG

The content in this document will be periodically updated to reflect the changes in the County environment and to capture industry best practices as the technology and standards continue to evolve.

DATE	NEW VERSION NUMBER	MODIFIED BY	DESCRIPTION OF CHANGE
03/01/2003	1.2	H. Kao (ISD)	1) Content revisions were made.
05/12/2003	1.3	R. Pittman (CIO)	1) Updated appendix E to add a sample of what information is required. 2) This final version was distributed at TSAB.
08/08/2003	1.4	R. Pittman (CIO)	1) Added section 7.0.1 Submittal of Forms Procedure. 2) Added this history log in section 1.0.1. 3) The document date is no longer being generated automatically by Microsoft Word

2.0 WIRELESS LAN DEPLOYMENT & OPERATION GUIDELINES

This Guideline was developed by Cyber Terrorism (CT) Security Engineering Team (SET) and is intended to address security issues related to remote network access and wireless network access in the County. This workgroup will produce recommendations that will fit the overall security framework, which will be formed based on the input of all workgroups within CT SET. The workgroup meetings are designed to provide a forum for collaboration among the team members, who are representatives from different organizations in the County. Through a consensus-driven process, the workgroup will produce recommendations and security guidelines that will help mitigate security risk in the County. The workgroup will identify security issues and determine their priorities according to the threat they present to the environment. The areas related to remote access and

wireless access in the environment that represent immediate threat to the County are addressed by the workgroup first.

As a part of the work under the Cyber Terrorism (CT) Security Engineering Team (SET), this paper emphasizes security risk mitigation related to WLAN. The aim is to provide a practical guide for WLAN by drawing from the proven practices and the knowledge gained in the industry. Each organization in the County, with the specific knowledge of its own business environment, will determine the appropriate capabilities for its requirements. As the industry evolves, WLAN standards and technology will continue to improve. These guidelines will be updated periodically to reflect the changes in the industry and to take into account the experience that is gained through the CT SET forum in the County.

3.0 WLAN OPENS UP YOUR IT ENVIRONMENT

There are three modes of WLAN operations. (1) WLAN Access Points (AP) are used to provide connection between LANs where physical infrastructure is not available. This type of networking is referred to as point-to-point (or point-to-multipoint) bridge mode of operation. (2) WLAN client stations communicate directly with each other on a peer-to-peer level. This type of networking is often formed on temporary basis, and is referred to as an "ad hoc" mode of operation. (3) The prevalent mode of WLAN operation is referred to as the "infrastructure" mode. In the infrastructure mode of operation the AP forms a bridge between the wired infrastructure and the wireless LAN. Client stations do not communicate on peer-to-peer basis. All communication between WLAN client stations or between WLAN client stations and any node on the wired network must go through the AP. AP's are not mobile; they are physically wired to the wired network infrastructure, hence the name infrastructure mode. The infrastructure mode is the dominant mode of operation in the County and, hence, the focus of these guidelines.

Functionally, WLAN may be used to either replace or to extend the LAN infrastructure. In most County organizations, WLAN are used in the infrastructure mode of operation. Whether you use it simply for extending connectivity beyond the physical boundary of your LAN, or for the flexibility of networking users without the constraint of a wire, WLAN expands your private network, and potentially expands your vulnerability to new kinds of security risk. The additional benefits you gain from WLAN must be balanced with the additional security burden you need to deal with. The policies and procedures governing the IT practices in your organization related to LAN deployments and operations should be the framework for determining the baseline requirements for WLAN. The current design guidelines, vendor selection process, and procurement procedures for network equipment also apply to WLAN. However, with WLAN, additional effort is required to cope with the risk associated with wireless communication.

WLAN presents new kinds of challenges to an organization. There is inherently less control over the integrity, reliability, and confidentiality of WLAN than you have with the wired LANs. The issues related to transmission contention, interference, and security risk associated with wireless communication require extra attention. Products based on the 802.11b standard dominate the industry today. 802.11b operates in the unlicensed 2.4GHz ISM (industry, scientific, medical) band as designated by FCC. Since it is not licensed, anyone may use it. Bluetooth, the short-range personal area network (PAN) technology also uses the 2.4GHz frequency spectrum. The FCC regulates the maximum transmission power and the bandwidth usage for each type of transmission in the ISM bands. For example, 802.11b uses a technique called direct sequence spread spectrum (DSSS) and Bluetooth uses a technique called frequency hopping spread spectrum (FHSS) for transmission. For each type of transmission, the FCC specifies the frequency range and the maximum power that is allowed.

The emerging 802.11a technology uses ISM band in the 5GHz range, which is treated the same way. No one has the right of way over the ISM frequency spectrum.

One characteristic of WLAN communication is that the AP's must broadcast their presence into the air regularly. This is a designed behavior of the AP according to the 802.11 standard. The management frames the AP's send out are referred to as beacons. Beacon frames are broadcasted without encryption. All client stations within the coverage area, whether they are legitimate clients or not, see the beacon frames broadcasted by the AP. The typical information the client can derive from the beacon frames are the service set identifier (SSID); the signal strength, the frequency channel, the MAC address, and even the location of the AP can be determined when a GPS is used. No hacking is required to learn about the details of an AP.

Between the AP and the client station, the reachable distance is proportionally increased with power (not to exceed 100mW internationally or 1W in the US) and inversely impacted by the speed of transmission. 802.11b may operate at 1Mbps, 2Mbps, 5.5Mbps, or 11Mbps. At 2Mbps and maximum power, the coverage distance is approximately 300 feet from the AP. However, industry experiments have shown that client stations equipped with high gain directional antennas may connect to WLANs over 25 miles away. One should realize that the physical boundary of the wired LAN, the AP, is where one's domain of control effectively ends. WLAN requires extra consideration in at least three areas: authentication, data encryption, and network integrity. Since the information is transmitted over an open medium, the data frames may be altered, authorized sessions may be hijacked, or imposters may impersonate the network to steal authentication credentials. Additionally, the types of denial-of-service attacks that might result from frequency interference, saturation, or jamming (intentional or unintentional) are difficult to prevent.

Despite the shortcomings, WLAN technology has gained wide acceptance across the industry. The emerging 802.11a (see Appendix A: WLAN Technology Primer) standard promises greater capacity and the 802.11i standard will provide solutions for many of the security problems associated with WLAN today. The technology is progressing and we need to move in alignment with the progress. One should recognize that the radio portion of the network is unsafe. The amount of security protection that is required will always depend on the service objectives. The current state of WLAN technology is neither good nor bad, it is only good or bad in the context of the business applications. The sensitivity, performance, and reliability of the business applications ultimately determine the design of the network infrastructure.

4.0 KNOW THE SECURITY REQUIREMENTS

IT security policy, explicit or implied, defines the rules that regulate how the County manages and protects its information and computing resources, and how to achieve security objectives. One of the policy's primary tasks for detecting signs of intrusion is to document important information assets and clarify the threats to those assets. When WLAN access points are introduced to a secure and trusted network in the County, additional considerations must be given to security issues. Specifically, there must be risk assessments to identify the impact WLAN access would have on the organization. Information assets must be inventoried. Hence the first priority is to examine the information resources that are worth protecting and then categorize them by the levels of security sensitivity.

Understand the consequences of security violations. Know the impact your organization has on the entire County when your network security is compromised. Considering the threat of cyber terrorism, what are the implications of a security breach in your network? If your network is connected to the County enterprise (data

centers and other departments) and is treated as a trusted entity by others, then a security breach in your network compromises the security of the entire enterprise.

WLAN security should be determined in the context of the organization's business. A practical solution will depend on the organization's ability to support it in its operating practices. How does one tell when there is a security violation? What types of features are embedded in the network infrastructure that will generate security alerts? Who in the organization will be responsible for enforcing the rules? What are the escalation procedures to resolve security problems in your organization? A sound security framework encompasses many policy and practice factors in addition to the features and functions embedded in the technology. WLAN will be an extension to your network and it will impose extra requirements for security because of the open nature of the technology.

5.0 KNOW THE BUSINESS DRIVERS

Think about the business reasons for WLAN before worrying about the technical issues such as coverage zones, frequency conflicts, and security vulnerabilities. Is WLAN for productivity gain, reducing cabling cost, or networking field service personnel? Once the business benefits and the technical challenges are understood, you can properly assess the merit of WLAN in your organization. What types of business functions in your organization warrant WLAN service? Where should you provide coverage and where should you not? What applications should be supported over WLAN? Who are the users of WLAN? What are their usage behaviors? Is there an alternative solution based on the existing wired infrastructure?

In general, when a wired connection is available it is always preferable to a wireless connection. With the security issues identified and other limiting factors such as reduced bandwidth availability, contention for a shared medium, and the unpredictable radio interferences, wireless solution should only be implemented where there is a legitimate business reason to do so. The cost of implementing a wired infrastructure alone is not a legitimate business reason for implementing WLAN except for temporary installations. There must be compelling business reasons for mobile computing.

Explore the deployment related questions after WLAN has been justified. Some basic questions are: What is the maximum number of users at a given service location? What is the maximum number of service locations required in a building? Are users from other County departments sharing the same service location or the same building? The reliability and security of WLAN services require extra planning and management effort because the transmission medium is open and unsecured, and the FCC does not license the transmission frequency.

6.0 DEPLOYMENT GUIDELINES

6.1.1 Considerations for Multi-tenant County Buildings

Special consideration must be given to the requirements in multi-tenant County buildings. In order to have WLAN reliability, integrity, and security there must be a joint effort among all departments sharing the same building to coordinate deployment and operation activities. Having one central IT management organization responsible for WLAN service in the building and accountable for enforcing a common usage policies will be the best way to proceed. Following are the main factors related to deployment.

6.1.2 Airwave usage

Within the County buildings the usage of airwaves shall be coordinated and managed by ISD or a central IT organization agreed to by all tenants in order to avoid unnecessary service degradation and exposure to security risk. If individual departments install their own AP's, they implicitly make claim of the shared airwave in the building without regard for the needs of other departments. Uncoordinated installation of WLAN's in a shared building will lead to excessive frequency interferences and degrade services for everyone. ISD or a central IT organization will control the airwave in the building. The "ad hoc" mode of WLAN operation will not be allowed. All WLAN operation shall be in the "infrastructure" mode only. Any unauthorized AP will be confiscated and removed from the building.

6.1.3 AP Management

ISD or an agreed upon central IT organization will manage the AP's in multi-tenant County buildings, and will have the responsibility to support WLAN communication for all departments in the building. AP devices that will be shared by multiple departments in the building will be deployed and operated to deliver a broader suite of functionalities than that of a single department. ISD or the central IT management organization, with clear responsibility for all AP's in the building, will help prevent unnecessary confusion among the departments. A central IT authority will coordinate the services and manage the ongoing operation more effectively.

6.1.4 Coverage Zone

WLAN coverage zones, "hot spots", in the multi-tenant County buildings will be determined according to the needs of every department in the building. The number of users in a given area and the number of coverage areas needed in the building must be determined in order to properly locate and configure the AP's. ISD or a central IT management organization shall consult each department in the building to identify their business drivers, applications, usage behaviors, and other designed requirements for the wired network infrastructures to determine a coverage zone that will serve all the tenants in the building.

6.1.5 AP Placement

The locations of AP placement will be determined according to the coverage zones required in the building. There should be special consideration for network security in selecting AP placement locations. Traditionally, firewalls are installed to defend the perimeters of the wired network, and they are monitored meticulously because the organization understands the potential risk outside. The organization considers the network outside the boarders unsafe because the outside environment is unpredictable and uncontrollable. Likewise, the environment outside the radio interface of the AP is unsafe; hence the installation of an AP implies opening up an entry point into the organization from a potentially unsafe territory. The placement location of an AP and the infrastructure behind it should be designed and managed to protect the interest of all tenants in the building as well as the security environment of the entire County.

6.1.6 AP Connection

The connection to the wired infrastructure in a multi-tenant County building should ensure that the AP has a path back to each department's LAN and application environment. In addition to ensuring the AP

supports connectivity to each department's backend environment, care must be given to the different needs of each department as dictated by their business drivers, application behaviors, bandwidth usage, security, etc. ISD or the central IT management organization shall consult all the departments in the building to understand their specific WLAN requirements in order to determine the proper connection point and the associated support infrastructure for the AP.

6.2.0 VLAN AND VPN FOR DISTRIBUTION

In a multi-tenant County building, all departments will share common AP's for WLAN communication. The distribution network behind the AP's is configured to deliver each user's traffic to the appropriate server environment where the department's applications reside. The application of interest for the particular user may be hosted locally in the building, in the ISD data center in Downey, in the department's own data center somewhere within the County, or outside the County's firewalls in the Internet. ISD or the central IT management organization needs to have broad capabilities and coverage for the entire County network in order to provide end-to-end transport service across geographically disperse locations. According to the unique requirements of each department, it might be necessary to support various levels of separation and protection for WLAN traffic. VLAN's will be used to separate user groups or departments in the building and VPN's in the Enterprise Network could be used in some situations to provide enhanced safeguard for transport to and from remote County locations. ISD or a central IT management organization, with the global view of interactions in the building, will create or recommend appropriate VLAN and VPN solutions for each tenant.

6.3.0 CLIENT DEVICE MANAGEMENT

Each department in a multi-tenant County building may purchase WLAN client devices independently. The devices, however, must be Wi-Fi compliant. For example, 802.11b standard based WLAN adapters for PDA's, Laptop PC's, or Desktop Workstations will be supported in the building. All client devices to be used in the building should be registered with ISD or the central IT management organization so they may be properly associated with the AP's in the building in order to support the functionality and security requirements.

6.3.1 Authentication

In order to minimize security risk, all access attempts to the WLAN should be authenticated at the device level as well as the user level. At the device level, the device MAC address, SSID, device name, and the encryption key may be used collectively to verify the identity of the device. At the user level, user ID and password should be authenticated against an authentication database, which may be an enterprise directory or a RADIUS (Remote Access Dial-In User Services) server. A client device will be granted access to an AP only upon a combination of device and user authentication. ISD or a central IT management organization needs to maintain a common user directory database in order to determine the access level and service profiles of WLAN users in the building, and grant them appropriate services.

6.3.2 Encryption

Each department in the multi-tenant County building might have different protection requirements for the data transmitted over WLAN. The transmission originates from WLAN might go through different

types of encryption and the actual end points of the encrypted tunnels might vary from one user to another. The vulnerability of WEP is well known in the industry and will not be sufficient for security protection generally. Additional capabilities such as user level authentication and dynamic encryption keys will be required to protect sensitive data. An encryption mechanism that provides a secured tunnel between the client station and the AP might be sufficient for some users, but others might require a VPN tunnel that extends all the way to the application servers, which may be a remote location across the Enterprise Network. ISD or a central IT management organization that has broad responsibilities across the County will be able to support a more comprehensive solution.

6.3.3 DHCP Server

After gaining access to the WLAN, the client devices need IP connectivity in order to communicate with the servers and applications, which might reside anywhere in the County. For security reasons, the IP subnet that is allocated to client devices should be different from the subnet allocated for AP management. The ability to manage address allocation based on unique user profiles gives IT management control over the WLAN traffic. The ability to manage address allocations, hence influencing routing and network reach ability, depends on the management of the DHCP (Dynamic Host Configuration Protocol) server. ISD or a central IT management organization that has global view of the entire networking environment should control the DHCP server and correlate its configuration with those in Switches and Routers in order enhance end-to-end connection service.

6.3.4 RADIUS Server

As a mechanism for managing user identities in the building, the profile of each WLAN user should be stored in an enterprise directory or a RADIUS server. Typically, a RADIUS server is used to authenticate users dialing into the network from remote locations. In addition to authentication services, it also provides the mechanism for controlling, monitoring, and accounting remote access activities. RADIUS serves the same functionalities for WLAN. ISD or a central IT management organization should manage identities of WLAN users on an enterprise directory or a RADIUS server and use RADIUS services to authenticate, monitor, audit, and log each client connection in order to ensure security.

6.3.5 Roaming Service

Within a shared building, WLAN users from different County departments may connect to the same AP. Since mobility in WLAN is limited to the Data Link Layer, WLAN clients need IP services in order to connect to the appropriate network resources. The design for roaming services will depend on a collection of other services: DHCP servers, DHCP relay on routers, RADIUS, cross-departmental directory database, etc. Both WLAN and the wired LAN infrastructure need to adapt to the special needs of the individual departments. The distribution network and the core network infrastructure behind the AP's must provide the necessary capabilities to support the different requirements. In addition to the transport requirements, authentication and encryption requirements must be addressed on multi-department basis. Since ISD has broad responsibilities for network infrastructures across the County, it will be in the best position to address the needs for multi-department roaming service.

6.4.0 CONSIDERATIONS FOR SINGLE-TENANT COUNTY BUILDINGS

County buildings that house a single tenant and are under the jurisdiction of a single management organization should be evaluated using the same criteria outlined for the multi-tenant situation above. The organization that is in charge of the building should coordinate and manage WLAN activities in the building. In order to have WLAN reliability, integrity, and security there should be one central IT management responsible for WLAN deployment and operation in the building. No business unit in the organization should install WLAN independently without collaborating with the central IT organization for the building. Following are identical factors as specified in the multi-tenant situation, except the task of implementation might be simpler because one department with one IT organization responsible for a smaller amount of services might encounter less obstacles in the process.

Airwave Usage
AP Management
Coverage Zone
AP Placement
AP Connection
VLAN and VPN for Distribution
Client Device Management
Authentication
Encryption
DHCP Server
RADIUS Server
Roaming Service

6.5.0 CONSIDERATIONS FOR NON-COUNTY BUILDINGS

A County organization that shares office space in a building that belongs to a non-County entity must observe the rules established by the building management. Even if no rule has been established for airwave usage in the building, the guidelines regarding airwave usage, AP management, coverage zone, AP placement, and AP connection, and roaming service must be evaluated using the same criteria as recommended above for the multi-tenant County buildings. Additionally, the design and management of the wired infrastructure that makes up the backbone for the AP's for the organization must meet County security requirements. The unique requirements for deployment and operation of WLAN to support an organization that shares non-County buildings need to be addressed on case-by-case basis with special consideration for the needs of other tenants in the building.

6.5.1 Configuration Guidelines

For practical reasons, the minimum configuration of WLAN infrastructure to support the appropriate level of security will be determined based on short-term, mid-term, and long-term requirements. Recognizing the realities of risk inherent in the current state of the technology, one should deploy WLAN products that serve today's needs and have the flexibility to adapt and grow as the technology continues to improve. While 802.11b technology has gained wide acceptance in the industry, developmental work continues in IEEE bodies and in the vendor communities to resolve the known problems and to enhance service capabilities. WLAN product life cycles are short. The following recommendations provide a baseline for County organizations to meet the minimum requirements for short-term, mid-term, and long-term security objectives. The configured parameters must be supported by the organization's operation practices as recommended in the next section. The ongoing management and operation of WLAN are integral parts of the solution. The following

configuration guidelines apply to any WLAN that directly or indirectly connects to the LAnet or the Enterprise Network.

6.5.2 Configuration for Short-term Requirements: Immediate implementation

1. No "ad hoc" mode is allowed, allow "infrastructure mode" operation only
2. Install AP's at a physically secured location
3. Provide basic device level authentication and encryption using WEP
4. Provide user level authentication
5. Unique SSID to distinguish WLAN
6. Create a unique name for each AP
7. Disable SSID broadcast
8. Enable a strong management password on each AP
9. Create separate IP subnets for AP management
10. Use DHCP server for client IP connectivity management
11. Restrict any unnecessary services: IP address and TCP port ranges
12. Create unique names to distinguish client devices
13. Use 128 bit WEP key for basic encryption services
14. Use MAC address filters on AP's to screen client devices

6.5.3 Configuration for Mid-Term Requirements: Scheduled no later than 8/2003

1. Provide device level plus user level authentication and encryption
2. Provide dynamic encryption keys to overcome weakness of WEP
3. Provide 802.1x, EAP-TLS or equivalent
4. Provide dedicated LAN segment or VLAN for AP backbone
5. Force all AP's to pass authentication to a central RADIUS server
6. Use VPN, Firewall, and VLAN infrastructure to protect the wired network from WLAN

6.5.4 Configuration for Long-term Requirements: Scheduled for 8/2003 forward

1. Provide central directory database for authentication services
2. All AP's pass authentication to the central directory database
3. WLAN security infrastructure correlates to other network-based and host-based security mechanisms in the enterprise such as firewalls, routers, and applications to support the overall anti-cyber terrorism framework in the County.

7.0.0 OPERATION GUIDELINES

WLAN should not be treated as a fragmented installation. WLAN components should be added to the network management system, and the operating practices covering fault management, configuration management, performance management, and security management should be analyzed for compatibility and consistency. Integrating WLAN components into a unified management platform that supports network infrastructure for the organization will facilitate asset management as well as policy management and enforcement. Security policies can be enforced effectively only when there is visibility across the entire network – client to host and everything

in between. The airwave in WLAN frequency ranges should be managed as a part of the organization's assets. If the IT management organization controls who may connect to the wired infrastructure and the associated resources, it should do the same for WLAN. If the IT management organization partitions LAN traffic in order to protect sensitive data from potential risk, it should do the same with WLAN.

The management and operation of WLAN should be a natural extension to the network management system of the organization. The day-to-day operating practices play a critical role in creating WLAN security solutions. Monitoring and auditing functions should support the features and security attributes deployed in WLAN infrastructures as recommended in the previous section. The operation should continue to adjust and update support for the capabilities that are deployed for the short-term, mid-term, and long-term requirements. The following operation guidelines apply to any WLAN that directly or indirectly connects to the LAnet or the Enterprise Network.

7.0.1 Procedure for Submitting the Required Forms

The AP's that have connectivity into the County's enterprise environment shall be registered with ISD Data Security. ISD Data Security will maintain a database of AP's. The database will be used to periodically survey County facilities in order to prevent rogue AP's. An AP that is not in the database will be disconnected and confiscated. The AP database will also be used as a part of the CERT knowledge base for discovering network attacks in case of a cyber-terrorism event.

Registration by all departments will also ensure that the guideline configurations have been met and thereby the overall enterprise wide security is maximized.

Appendices D and E have Wireless LAN Security Checklist and Access Point Registration Form, respectively. Both documents are required to be submitted. The following procedure should be used for registering your wireless access points:

1. Review and adhere to the standards in appendix D
2. Complete the form in appendix E
3. The Chief Information Office, Chief Information Security Officer (CISO) will be overseeing this activity. Appendices D and E should be submitted to the following address:
   a) Send to Al Brusewitz, CISO, Chief Information Office, 9150 East Imperial Highway, Mail Stop 23, Downey CA 90242. For electronic document submission please send to: abrusewitz@cio.co.la.ca.us
   b) Also send a copy to Robert Pittman, Assistant CISO to the same address indicated in item a. For electronic document submission please send to: rpittman@cio.co.la.ca.us
4. ISD Data Security Division will require both documents for review and verification of compliance. Please complete appendices D and E and submit to:
   a) Send to Valerie Glass, Division Manager, ISD Data Security, 9150 East Imperial Highway, Mail Stop 25, Downey CA 90242. For electronic submission please send to: vglass@isd.co.la.ca.us

7.0.2 Operation for Short-term Requirements: To be implemented immediately

1. Register clients by user name, device name, and MAC address
2. Maintain an inventory of SSID, Client name, MAC address, and AP by building

3. Perform a risk assessment on AP's and associated resources
4. Monitor and capture patterns and trends of client-to-AP associations
5. Generate client association reports by client names and MAC addresses
6. Remove unauthorized AP's and unregistered clients from the network
7. Coordinate WEP key renewal every 30 days

7.0.3 Operation for Mid-Term Requirements: To be implemented no later than 8/2003

1. Manage profiles of WLAN users on a centralized RADIUS server
2. Centralized the management of AP configurations for all AP's
3. Support event notification on AP's – fault, threshold, log-in attempts, etc
4. Collect access and usage statistics on the RADIUS server
5. Generate audit logs and reports for security assessment
6. Generate security alerts on irregular events

7.0.4 Operation for Long-term Requirements: To be implemented 8/2003 forward

1. Manage all user profiles on an integrated directory database
2. AP's are included in the intrusion detection framework for the enterprise
3. Integrate WLAN management into the overall network management system
4. Keep up with FCC regulations on WLAN and the industry reports on security issues and the best practices to mitigate WLAN related security risk.

8.0 CONCLUSION

Know the benefits of WLAN in the context of the current state of the technology. Security standards are evolving and new products continue to emerge in the market place. Airwaves must be shared and unmanaged contention will degrade services for everyone. Product life cycles will be short. Know your security requirements in the context of the overall County requirements. Since the organization and network do not exist in isolation, compromising security also poses potential threat on other County organizations that connect to your network and trust it as a secured environment. The prudent approach is to deploy WLAN by following the mainstream practices in the industry today, and prepare network infrastructure with the flexibility to change.

Treat WLAN security as a component of the overall anti-cyber-terrorism initiative in the County. WLAN security is a part of the organization's IT security framework, which should include policies for resource allocation, prioritization, and protection. The enforcement of WLAN related security at different layers (application layer, operating system layer, network layer, and physical layer) should be an integral part of the organization's overall security framework. For example, the establishment of a central directory database for user identity management, VLAN and VPN for data confidentiality, and intrusion detection systems for network defense are inter-dependent mechanisms that collectively support policy enforcement.

Take the prudent approach and deploy practical WLAN solution without compromising security requirements. Justify WLAN based on your business drivers, and implement it based on the knowledge of the pros and cons outlined in these guidelines. Deploy it according to the short-term, mid-term, and long-term configuration guidelines. Update your network management system and operating practices to support it as you move from short-term to mid-term to long-term solutions.

APPENDIX A: WIRELESS LAN TECHNOLOGY PRIMER

IEEE 802.11: IEEE 802.xx is a set of specifications for LANs from The Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared. 802.11b uses DSSS to provide 11 overlapping channels across the 83 MHz within the 2.4 GHz frequency spectrums. Within the 11 overlapping channels, there are three 22 MHz non-overlapping channels. Since there are three channels that do not overlap, it is possible to use three AP's simultaneously to provide an aggregate data rate of the three non-overlapping channels. The emerging standard, 802.11a, uses 5 GHz spectrum to achieve data rates as high as 54 Mbps. 802.11a uses a type of frequency-division multiplexing called orthogonal frequency-division multiplexing (OFDM). The available bandwidth is divided into multiple data carriers. The data to be transmitted is then divided between the data carriers and treated independently from the others. The current expectation for finalization of 802.11a by the IEEE is mid 2003. Anther emerging standard is 802.11g, which is also expected around mid 2003. Product vendors will probably release 802.11g adapters and access points in late 2002 or early 2003. 802.11g standard is an extension to 802.11b. It will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM technology. Because of the backward compatibility, an 802.11b radio adapter will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range.

The success and the continual momentum of WLAN technology is attributed to a nonprofit, vendor neutral organization known as Wireless Ethernet Compatibility Alliance (WECA). WECA provides a branding for the 802.11 technologies known as Wi-Fi (wireless fidelity). A Wi-Fi compliant device must pass the interoperability testing in WECA laboratory, and is assured compatibility with all other Wi-Fi certified products in the market.

MAC (Medium Access Control): In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packets formats and addressing, and error detection.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance): CSMA/CA is the principle medium access method employed by IEEE 802.11 WLANs. It is a "listen before talk"; method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously. Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection): The LAN access method that is used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is free. If it is not, it waits a random amount of time before retrying. If the network is free and two devices access the line at exactly

the same time, their signals collide. When the collision is detected, they both back off and each waits a random amount of time before retrying.

ISM (Industry, Scientific, Medical) Band: The frequency bands allocated for general usage without FCC license: 902 MHz to 928 MHz, 2.4 GHz to 2.4835 GHz, and 5.725 GHz to 5.850 GHz. For example, 802.11b and Bluetooth technology operate in the 2.4 GHz band, and 802.11a technology operates in the 5 GHz band.

DSSS and FHSS: Wireless LAN products are available in three different technologies -- direct-sequencing spread-spectrum (DSSS), frequency-hopping spread-spectrum (FHSS) and infrared. DSSS and FHSS are spread-spectrum techniques that operate over the radio airwaves in the unlicensed ISM band (industrial, scientific, and medical). DSSS uses a radio transmitter to spread data packets over a fixed range of the frequency band. FHSS uses a technique by which the signal transmitted hops among several frequencies at a specific rate and sequence as a way of avoiding interference. **WECA's** focus is on the use of DSSS for 11 Mbps high rate wireless LAN communications.

AP (Access Point): A hardware device, or software used in conjunction with a computer, that serves as a communications "hub" for wireless clients and provides a connection to a wired LAN. An AP can double the range of wireless clients and provide enhanced security.

Ad-Hoc Mode: A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is where PCs communicate with each other through an AP. See AP and Infrastructure Mode.

Infrastructure Mode: A client setting providing connectivity to an AP. As compared to Ad-Hoc Mode where PCs communicate directly with each other, the clients that are set in Infrastructure Mode all pass data through a central AP. The AP helps mediate wireless network traffic in the immediate neighborhood and provides communication with the wired network. See AD-Hoc and AP.

Roaming: Moving seamlessly from one AP coverage area to another with no loss in connectivity. The 802.11 specifications do not stipulate a particular mechanism for roaming. Industry vendors choose their own algorithm for WLAN clients to make roaming decisions. AP sends out periodic management frames known as beacons. Beacons contain AP information such as service set identifier (SSID), support data rates, whether the AP supports frequency hopping or direct sequencing, and bandwidth capacity. The actions taken in the roaming process may differ from one vendor to another. Generally, the client may reinitiate a search for an AP in the same manner it started originally, or it may reference a table that was built during the previous association. Since the roaming techniques are vendor specific, roaming between AP's of different vendors may encounter compatibility problems or extended roam times.

WEP (Wired Equivalent Privacy): WEP data encryption is defined by the 802.11 standard to deter (1) access to the network by "intruders" using similar wireless LAN equipment and (2) capture of wireless LAN traffic through eavesdropping. WEP allows the administrator to define a set of respective "Keys" for each wireless network user based on a "Key String" passed through the WEP encryption algorithm. Access is denied to client stations that do not have the matching key string as coded in the AP.

Bluetooth: As a potential technology contender as well as a source of communication interference to 802.11 WLAN, Bluetooth is a short-range (about 10 meters) wireless technology operating in the same 2.4 GHz ISM band. Bluetooth wireless specification supports both data and voice applications. Operating in the same frequency spectrum, the radio uses spread spectrum, frequency hopping, and full-duplex signal at up to 1600

hops per second. The signal hops among 79 frequencies at 1 MHz intervals, which provides high degree of immunity to interferences.

In comparison to 802.11 WLAN, Bluetooth has much shorter range and lower throughput, which also means lower power consumption. The significantly lower power consumption makes it more ubiquitous than 802.11. For close-range personal area network, Bluetooth capabilities can be installed in personal digital assistants, cellular phones, pagers, printers, scanners, digital cameras, and home appliances - the original role was to replace short-range cables.

Antenna: Based on the coverage zone required, an antenna type can be selected for its radiation pattern. The radiation patterns may be omni-directional, bi-directional, or unidirectional. Omni-directional antennas are the vertical antennas that provide a radiation pattern like a donut shape, which is good for covering a large area horizontally. Vertically, the coverage provided by a vertical antenna is rather limited. Bi-directional antennas are the dipole antennas that provide a radiation pattern like a figure eight, which is good for covering corridors. Unidirectional antennas are the yagi or parabolic antennas that radiate in a single direction, which is good for setting up point-to-point links between buildings.

APPENDIX B: SURVEY QUESTIONS RELATED TO WIRELESS LAN

1. Does your organization have WLAN?
2. Do you have 802.11b WLAN?
3. Do you have 802.11a WLAN?
4. Do you use WLAN in peer-to-peer mode (ad hoc mode) of operation?
5. Do you use WLAN in point-to-point bridge mode of operation?
6. How many WLAN access points do you have?
7. Do you use 128bit WEP on your WLAN access points?
8. How many WLAN users do you have?
9. Do you implement MAC filters on WLAN access points?
10. Do you implement user level authentication on WLAN?
11. Do you manage WLAN users on central RADIUS server for authentication?
12. Do you support dynamic encryption over WLAN?
13. Do you have an established operating procedure for WLAN?
14. Do you perform periodic audits on WLAN access points?
15. Do you have a dedicated VLAN for WLAN access points?
16. Do you have dedicated IP subnet for WLAN?
17. Do you support VPN over WLAN?
18. Do WLAN users access IT resources located locally?
19. Do WLAN users access IT resources in County data centers?
20. What applications WLAN users are using?
21. What client devices WLAN users are using?
22. Who are your WLAN product vendors?
23. Do you measure WLAN frequencies and coverage?

APPENDIX C: POTENTIAL PROBLEMS ASSOCIATED WITH WIRELESS LAN

1. **"Rogue" Access Points**
   AP deployment in the organization without the IT department's knowledge is a problem. The relatively inexpensive WLAN components make it possible for many department staff, who traditionally depend on the IT department to supply them with technology, to buy AP's and client adapters themselves. WLAN devices are relatively inexpensive and little technical expertise is required to get them up and running in the factory default mode of operation. Unfortunately, the department staff can buy the devices under their budget authorities and can justify the benefits of WLAN, but they may not be aware of the security implications for the organization.

2. **AP's with factory default configuration**
   Many AP's are deployed with default configurations, which opens up avenues for un-authorized users to enter the network. There are results published in the Internet that majority of AP's are installed with minimum modifications to their factory default configuration. They either have not activated Wired Equivalent Privacy (WEP) encryption or simply use the default key as used by vendors coming out of the box. Even if there is no security concern for unauthorized users accessing the network, there are at least two problems that might result from such open access. Legitimate users might be denied of service because bandwidth is deliberately or unnecessarily consumed by unauthorized users, or hackers might use the network as a launching platform for cyber terrorism activities. Either could cause financial or legal challenges for the organization.

3. **Spoofing of client station MAC addresses**
   Network transmission based on 802.11 does not authenticate data frames. Every data frame has a source address but there is no mechanism to guarantee that the station sending the frame actually transmits the frame. There is no protection against forgery of the source address of the frame. Hackers can observe the MAC addresses of the stations in the network and use them for launching illegal activities. Requiring the users of the client stations to authenticate themselves before entering the network may mitigate this type of risk.

4. **Risk associated with traffic eavesdropping**
   Network transmission based on 802.11 does not protect data traffic against eavesdropping. The headers of data frames are transmitted in the clear, and are visible to anyone with a wireless network analyzer. WEP encryption protects the data to some extent but the management and control frames are not protected. The vulnerability of WEP is well publicized. The industry is actively working on standards to strengthen 802.11 securities and overcome the shortcomings of WEP. In the mean time, product vendors have introduced interim solutions such as using WEP in conjunction with key management protocols to change the encryption key on regular short intervals, which makes it impractical for attackers to decode. If WLAN is used to transmit sensitive data or to connect to internal networks, then stronger protection mechanism must be deployed at or closer to the data sources. A more comprehensive solution for authentication and encryption should be deployed for greater security.

5. **Service constraints**
   WLAN brings about new types of denial-of-service attacks, not necessary caused by malicious intent. Operating in the unlicensed frequency spectrum, no one has the right of way. The radio capacity can be overwhelmed by the traffic coming from the wired LAN or from excessive number of WLAN client stations trying to use the service at the same time. Or an attacker might disable the network by simply

sending a large amount of traffic on the same radio channel used by the AP. Other types of equipment (see Appendix A: WLAN Technology Primer) operating in the same frequency spectrum will interfere with WLAN integrity if they are in the same area. Perform regular auditing and traffic trending analysis will help the organization to plan and architect solutions to minimize service constraints.

APPENDIX D: WIRELESS LAN SECURITY CHECKLIST

Month:_____ Date:_____ Year:_____

Organization Name: _____
Contact Information: _____
Responsible Manager:_____ Signature:_____

SHORT-TERM REQUIREMENTS – To be implemented immediately		
CONFIGURATION	**Mandatory**	**Recommended**
1. "Infrastructure Mode" operation only. No "Ad Hoc Mode" is allowed	x	
2. AP's are installed at physically secured locations	x	
3. Provide basic device level authentication and encryption - WEP	x	
4. Provide user level authentication	x	
5. Create unique SSID to distinguish Wireless LAN	x	
6. Create unique name for each Access Point	x	
7. Disable SSID broadcast	x	
8. Enable strong management password on AP's	x	
9. Create separate IP subnet for AP management	x	
10. Use DHCP server to manage and control client IP addresses	x	
11. Restrict any unnecessary services: IP addresses and TCP ports	x	
12. Create unique names to distinguish client devices	x	
13. Use 128 bit WEP key for basic encryption services	x	
14. Use MAC address filters on AP's to screen client devices		x
OPERATION		
1. Register clients by user name, device name, and MAC address	x	
2. Maintain inventory of SSID's, client names, MAC addresses, and AP's	x	
3. Perform risk assessment on AP's and associated IT resources	x	
4. Monitor and capture patterns and trends of client-to-AP associations	x	
5. Generate client-AP association reports showing client names and MAC	x	
6. Remove unauthorized AP's and unregistered clients from network	x	

7. Coordinate WEP key renewal every 30 days		x

MID-TERM REQUIREMENTS – To be implemented no later than 8/2003		
CONFIGURATION	**Mandatory**	**Recommended**
1. Provide device level and user level authentication & encryption	x	
2. Provide dynamic encryption keys to overcome the weakness of WEP	x	
3. Provide 802.1x, EAP-TLS or equivalent	x	
4. Provide dedicated LAN segments or VLAN for AP backbone	x	
5. Force all AP's to pass authentication to a central RADIUS server	x	
6. Use VPN, Firewall, and VLAN infrastructure to protect wired network from WLAN	x	
OPERATION		
1. Manage profiles of WLAN users on a central RADIUS server	x	
2. Centralize the management of configuration of all AP's		x
3. Provide support for event notification on AP's – fault, log-in attempts, etc	x	
4. Collect access and usage statistics on RADIUS server	x	
5. Generate audit logs and reports for security assessment	x	
6. Generate security alerts on irregular events		x

LONG-TERM REQUIREMENTS – To be implemented 8/2003 forward		
CONFIGURATION	**Mandatory**	**Recommended**
1. Provide central directory database for authentication services		x
2. All AP's pass authentication to central directory database		x
3. WLAN security infrastructure correlates to other network-based and host-based security mechanisms in the enterprise such as firewalls, routers, and	x	

applications to support the overall anti-cyber terrorism security framework in the County		
OPERATION		
1. Manage all user profiles on an integrated directory database		x
2. AP's are included in the intrusion detection framework for the enterprise	x	
3. Integrate WLAN management in the overall network management system	x	
4. Keep up with FCC regulations and industry reports on security issues and best practices to mitigate WLAN related security risk		x

APPENDIX E: ACCESS POINT REGISTRATION FORM

ACCESS POINT REGISTRATION						
AP Name & Type		**MAC Address**	**IP Address**	**Power Out/ Channel**	**AP Location**	**Installation Date**
1.	Cisco 1200	001122334455	00.000.00.0	100mW/CH 6	Telco Room L-40 3rd Floor 1000 Wireless Highway Signal, CA 90000	4-8-03
2.						
3.						
4.						
5.						
6.						
7.						

Remarks: New install. Will be using directional antennas.

Contact person: John Aironet
Address: 1012 West Temple Street
City: Los Angeles
Telephone No.: (000) 000-0000
Email: j_aironet@co.la.ca.us
Date: April 30, 2003

Authorizing Manager/Department Information Security Officer (DISO) signature:

Appendix D:
Communications/Low Voltage Specification for County of Los Angeles Public Library

COUNTY OF LOS ANGELES
INTERNAL SERVICES DEPARTMENT

INFORMATION TECHNOLOGY SERVICE
PREMISES SYSTEMS ENGINEERING

COMMUNICATIONS/LOW VOLTAGE SPECIFICATION FOR

COUNTY OF LOS ANGELES PUBLIC LIBRARY

SPECIFICATION FOR

COMMUNICATIONS / LOW VOLTAGE

Issued
March 18, 2003

Contact:
Dana Scott, Telecommunications Systems Engineer
1112 N. Eastern Avenue, Los Angeles, CA 90063
(323) 267-3152

PART 1 GENERAL

1.1 SCOPE

Items of work included in this Section, described in detail in PART 3. Also refer to attached typical drawings and cut-sheets as required.

Furnish and install a complete and functional system consisting of the following components/sub-systems as indicated (checked) below:

Req'd	System Component/Sub-System	Pertinent Specifications	Page #
☐	Special Conditions	Para. 1.2	
☐	Telephone Rooms	Para. 1.6	
☐	Definitions	Para. 1.6.1	
☐	Telecommunications Rooms	Para. 1.6.2	
☐	System & Auxiliary Equipment Pre-installation Requirements	Para. 3.1	
	Building Systems		
	Security	Para. 3.2	
☐	Intrusion Detection and Alarm	Para. 3.2.1	
☐	Card Access System	Para. 3.2.2	
☐	Restroom Door Release	Para. 3.2.3	
☐	Door Phone	Para. 3.2.4	
☐	Para. 3.2.5		
☐	Public Address	Para. 3.3	
	Video	Para. 3.4	
☐	CCTV	Para. 3.4.1	
☐	MATV	Para. 3.4.2	
☐	SATV (Satellite)	Para. 3.4.3	
☐	CATV (Cable Access)	Para. 3.4.4	
☐	Teleconference	Para. 3.4.5	
☐	Video Conference	Para. 3.4.6	
	Cabling System	Para. 3.5	
☐	Station (Voice/Data)	Para. 3.5.1	
☐	Workstation Outlets	Para. 3.5.2	
	Distribution Cabling	Para. 3.6	
☐	Voice Cabling	Para. 3.6.1	
☐	Fiber Optic Cabling	Para. 3.6.2	
☐	Cable Testing (Copper and Fiber)	Para. 3.7	
	Voice/Communications Systems	Para. 3.8	
☐	Nothern Telecom Norstar Compac ICS	Para. 3.8.1	
☐	VoiceMail	Para. 3.8.2	

Meeting Room ---------- Para. 3.9
☐ Public Address ---------- Para. 3.9.1
☐ Data/Video Projection ---------- Para. 3.9.2
☐ Projection Screen ---------- Para. 3.9.3

☐ Equipment Racks/Mountings ---------- Para. 3.10

1.2 SPECIAL CONDITIONS

In addition to all stipulations in other portions of the general specifications, all concerned trades shall comply with the following special conditions that directly pertain to communications and security systems:

A. Contractor Qualifications

The specified equipment shall be furnished and installed by a contractor who can show proof of having satisfactorily engineered and installed comparable systems within the past five (5) years, and who holds all legally required licenses, including General Electrical C-10 and Communication C-61 licenses.

Security system contractor must be an authorized, certified, installing dealer for Radionics, regularly engaged in the supply of security control systems, and must have occupied an established office for a period of not less than three years prior to bid date within the Project's geographic market area. The Radionics Dealer number must be supplied and verified prior to commencing work.

B. Parts Availability

The contractor shall confirm that within a reasonable distance of the job site, there is an established agency which stocks a full complement of parts, offers service during normal working hours on all equipment to be furnished and will supply parts to the County without delay and at reasonable cost.

C. Continuous Duty Operation

All individual components and composite systems shall be designed for continuous operation without undue heating or change in rated values and shall be properly fused.

D. Compliance with Codes

All work shall be done in accordance with latest applicable edition of National Electrical Code and all regulations, laws, safety orders, ordinances or codes of State and local authority, whichever exceeds, having the jurisdiction. Wherever requirements in the specifications exceed those of the ordinances or codes, specifications shall govern. Nothing in the plans and specifications shall be deemed as authority to violate any of the ordinances or codes.

1.3 SYSTEMS RESPONSIBILITY

The contractor shall furnish and install all non-specified equipment required to make each system fully functional as per stated intent and description, without additional cost to the County.

1.4 WARRANTY

A. All equipment and systems shall be warranted by the contractor for a period of one year following acceptance by the County. The warranty shall include parts, labor, prompt field service, and pick-up and delivery at no cost to the County. If repair of a defect cannot be affected during the initial response, every effort shall be made by the contractor to promptly correct the defect including air shipment of repair parts and replacement of the next larger assembly. **Response to initial call shall be accomplished within four (4) hours.**

B. Routine non-warranty maintenance shall be performed by the County. Neither this maintenance nor emergency repairs made by qualified County technicians shall void the warranty.

C. During the warranty period, the contractor shall respond only to calls for service made by ISD or designated Library Representative and shall keep the Department fully informed as to problems which develop in equipment or systems and as to steps the contractor has taken to rectify those problems. **Response to initial call shall be accomplished within four (4) hours.**

1.5 DATA TO BE SUBMITTED BY THE CONTRACTOR

A. Submittal Format

1. Submittal shall be furnished in an 8 ½" x 11" format in 3-ring loose-leaf binders. The cover and the title page shall bear the project name, capital project number, specification number, name of contractor and date. The document shall have a table of contents and page numbers on each of the pages including brochures and drawings.

2. Drawings shall be no larger than 34" x 22". Drawings larger than 8 ½" x 11" shall be folded to 8 ½" x 11" so that the drawing's name and page number are visible and can be unfolded without being removed.

3. Reproduced material shall not be subject to fading by light or heat and shall have high contrast for easy reading.

B. Preliminary Submittal

Within 30 days after contract award and prior to purchase of any equipment, the contractor shall submit five (5) copies of a Preliminary Submittal for review and approval. Three (3) copies to the Library Capital Project Section and two (2) to the ISD Telecommunications Systems Engineer. The submittal shall consist of the following:

1. Proposed material list including manufacturer's name, model number and technical data for all equipment the contractor proposes to install. Items shall be identified by specification section and paragraph number. The technical data shall consist of copies of factory issued catalog sheets or brochures, which give ratings and specifications for the proposed items.

2. Single line system diagram identifying and showing interrelationships between equipment items and how they are interconnected.

3. Shop drawings showing details of fabricated items, rack elevation drawings, console arrangements and schematics of custom designed items.

4. Statement describing exceptions being taken, if any, to the specifications wherein the submitted equipment or design varies from that originally specified.

5. If the contractor fails to list a particular variance and his submittal is accepted, but subsequently is deemed by the County to be unsatisfactory because of an unlisted variance, the contractor must replace or modify such equipment at once and without cost to the County.

6. For any exceptions that are not approved by County, contractor shall resubmit the information in complete compliance with the specifications and drawings.

C. Record (As-Built) Drawings

1. Record drawings shall be made on separate clean blueline prints of the electrical drawings issued by the County or Architect and shall be reserved for the purpose of showing work as actually installed, including accurately dimensioned locations of all conduit stub-outs and pull boxes, routing of all conduits extending from or between buildings and locations of all telecommunications equipment not installed according to drawings.

2. Drawings shall be kept up to date with neat and legible annotations made thereon daily as work proceeds, showing work as actually installed. Additional sheets may be attached to show greater detail. Drawings shall be available at all times for inspection and shall be kept on the job at a location designated by the County.

3. Contractor at his option may use an additional set of drawings for daily field annotations. This set of drawings shall be kept at the site.

4. Final record drawings shall be submitted with floor numbers, room numbers, panel directories and all other identification necessary to conform to number designations for occupancy rather than to construction numbers. All buried conduit and/or underground conduits stubs intended for future extension shall be accurately shown as to depth and exact measurement from a permanently established landmark, such as building or structural features.

5. On completion, record drawings shall be signed, dated and returned to the County for inspection and approval before acceptance of any work.

6. Provide three (3) sets of drawings to Library Capital Projects Section and one (1) set to ISD Telecommunications Systems Engineer.

D. Final Submittal

Three (3) complete sets of the Final Submittal including a full set of the drawings on vellum shall be delivered to the Library Capital Projects Section and two (2) complete sets to the ISD Telecommunications Systems Engineer prior to acceptance tests and as a condition for final payment for the project to the contractor. It shall include all the information necessary to maintain each system, and shall consist of the following:

1. Operators Instructions (as applicable).

2. Factory-issued Service Manuals for each piece of equipment installed. The manuals shall contain complete parts lists, detailed schematics, circuit descriptions, maintenance procedures and trouble-shooting methods. In the event such manuals are not available from the factory, it shall be the responsibility of the contractor to compile and submit the required information.

3. A System Manual for each system furnished. This manual shall complement the above service manuals with all necessary additional information unique to the system that is not otherwise provided, such as a list of applicable service manuals, options selected, jumper or strapping choices, modifications, and detailed wiring information.

4. Record Drawings (see Paragraph 1.5, C.5).

5. One (1) electronic copy of communications drawings in AutoCAD 14 format shall be delivered to Library Capital Project Section and to County ISD Telecommunications Systems Engineer

E. Addresses

1. Library Capital Projects Section
7400 E. Imperial Hwy
Downey, CA 90242

2. ISD Telecommunications Systems Engineer
1112 N. Eastern Ave
Los Angeles, CA 90063

1.6 TELECOMMUNICATIONS ROOMS

To complete the installation, testing and cut-over of the telephone and other sub-systems in a timely manner, the contractor shall give a high priority to completing ALL of the following as soon as possible and no later than four (4) weeks prior to the scheduled completion target date. Library Capitol Projects Staff and ISD Telecommunications Engineer also require immediate notification of any changes in the target date. Failure to comply with these conditions can and will result in communications systems in-service, and occupancy, delays. Refer to typical drawings and cut-sheets as required.

At no time will air conditioning units, condensate lines, water heaters, or any type of water lines, except fire sprinklers as required by code, be placed above any telecommunications room. No exceptions will be considered.

A. Communication Rooms Designations

1. **Building Entrance Facility Room (BEFR) (Formerly designated as MPOE)**
The communications cables from the local telephone company, the Minimum Point Of Entry or MPOE, are terminated in this room. It will house any telephone company equipment necessary to provide service to the County. This room may be included in the MCR if the Library is the only facility to be serviced from it.

In the case of a multi-tenant facility, this room will not be accessed through the Library. At no time will Library voice or data equipment be placed in this room.

2. **Main Communications Room (MCR)**
This room houses the Telephone system and main data communications equipment. The telecommunication cables from the BEFR, close workstations (as designated by ISD Telecommunications Systems Engineer), and TR's (if necessary), are terminated here. Intrusion Alarm equipment, Card Access System equipment, Paging equipment, etc. is housed in this room.

The MCR shall be located in the building in such a way that it is assessable **only** from the Library Staff workroom. Additionally, it shall be placed such that no data cabling, when installed and terminated, will exceed **275 feet** or **current EIA/TIA Standard.**

The MCR shall be equipped with furniture to provide a worksurface for technical staff. This may be in the form of a fully supported drop down worksurface. This should be at a height that is comfortable to work at standing. A "bar-type" stool shall be provided for sitting. It will also be equipped with an 18" deep bookshelf about the worksurface. The length may be determined int the field. If the size of the room permits, a desk and chair should be provided in place of the drop down worksurface.

3. **Telecommunications Rooms (TR) (Formerly designated as IDF)**
The ISD Telecommunications Systems Engineer along with appropriate Library Staff will determine is additional Telecommunications rooms are required. If required, the room shall be designated TR 1.2 for the first room on the first floor and TR 2.1 for the first room on the second floor, and so on. These rooms will house data communications equipment and cable terminations as required. The telecommunications cables from close workstations, as designated by ISD Telecommunications Systems Engineer, will be terminated here. It will also include Intrusion Alarm and Card Access equipment as necessary.

B. Air Conditioning

The MCR shall be provided with 24 hour, 7day air conditioning. Under normal operating conditions, a separate duct zone connected from the main building system shall provide **COOL AIR ONLY** in the MCR. If the main system fails to operate or maintain the required ambient temperature, a standby emergency system shall be automatically activated. Both systems shall be provided and installed with separately controlled

thermostats. The MCR shall NOT be under the control of any building energy conservations systems (BEAS). A temperature of 70 degrees Fahrenheit and a relative humidity range of 40% to 60% shall be maintained at all times. Before ANY communications equipment can be activated, a live test of the air conditioning system shall be conducted in the presence of the ISD/Telecommunications Systems Engineer or his/her designee.

NO air conditioning units (HVAC), condensate lines, water heaters, or types other water lines other than fire sprinklers as required by code, may be mounted directly above any MCR or Telecommunications Room (TR) unless otherwise approved in writing by the ISD Telecommunications Systems Engineer. In multi-story buildings, where TR's are placed directly above MCR's, or other TR's, (i.e. building risers) air conditioning/heating vents and ducts shall not be placed in the ceiling space directly under the TR.

C. Electrical Requirements

Install dedicated and isolated 20 amp electrical outlets, one (1) outlet (4 plugs) per circuit, in the MCR and IDF as shown on the plans.

D. Fire Protection

Provide a smoke detector and a high temperature sensor in the MCR and IDF, connect them to the fire alarm panel as two different zones. A fire extinguisher, of the type recommended for use on the electrical fires, shall be installed on the wall just inside the door, where it can be reached without completely entering the room. If the building is equipped with fire protection, all Telecommunications Rooms, shall have a Pre-Action System.

E. Backboards

Install fire-retardant, 3/4 inch plywood backboards covering all walls, from the floor to above the ceiling grid. Backboards shall painted off-white.

F. Door Locks

Install a door lock mechanism for all Telecommunications Rooms, keyed separately from all other keys.

G. Lighting

Lighting intensity in all Telecommunications Rooms shall be 90-100 foot-candles at 36 inches above finished floor. The bottom of lighting fixtures shall be 9 feet above finished floor.

G. Grounding

The grounding in all Telecommunications Rooms shall be a #2/0 AWG insulated ground cable from main building ground and terminate on a ground bar. See detail drawings.

I. Flooring

Coordinate with architectural plans and provide Anti-static vinyl flooring, Armstrong Static Dissipative Tile (SDT) Excelon Resilient Tile Flooring, or approved equivalent, in all Telecommunications Rooms. Anti-static vinyl flooring must be grounded to main building ground.

PART 2 PRODUCTS

2.1 MATERIALS AND EQUIPMENT

All materials and equipment shall be new, unused and manufactured within eighteen months prior to installation. Where applicable, all materials and equipment shall be listed by Underwriters Laboratories.

2.2 EQUIVALENT MATERIALS AND EQUIPMENT

Manufacturers' names and model numbers are used herein only as a means of establishing standards of quality and performance. Comparable equipment of standard manufacture and established reputation, which meets the requirements outlined above, may be submitted to ISD Telecommunications Systems Engineer for approval. Equipment of the following manufacturers may be used if it meets or exceeds parameters of the specified equipment.

A. Intrusion Alarm - Radionics
B. Access Control System – Hirsch/HID
C. Door/Window Sensors – Sentrol
D. Sirens – Sentrol
E. Photo Electric Beam Motion Detectors – Detection Systems
F. Cable – Superior Essex, Belden, West Penn, Berk-Tek, General
G. Panic Button – Suspicion, Edwards, Soundolier,
H. Paging Amplifier – Bogen
I. Community Room Public Address – TOA, Rauland
J. Loudspeaker/Transformer – Soundolier, Rauland, Quam
K. Loudspeaker/Enclosure/Baffle – Soundolier, Bogen, Dukane
L. Volume Control – Soundolier, Lowell, Dukane, Quam, Bogen
M. Distribution Amp – Pico Macom
N. Public Area and Emergency Exit Doors Panic Hardware – Von Duprin Series #99, Series #33 or Detex.
O. Door Bell/Door Phone – Viking

PART 3 SYSTEMS

3.1 SYSTEM & AUXILIARY EQUIPMENT PRE-INSTALLATION REQUIREMENTS

Electrical contractor shall install station conduits, riser conduits, cable trays and conduit hardware as shown on the drawings and according to procedures described under heading Part 4. H. Conduit.

The Telecommunications Rooms shall be constructed as shown on the drawings and according to procedures described under heading Part 1.6. HVAC system in the MCR

shall be operational 24-hour, 7 days a week. The heat dissipation of the communications equipment in the MCR is about 20,000 BTU.

General contractor shall coordinate with cable contractor for the cable installation and schedule.

Ceiling contractor shall be responsible for removal and replacement of ceiling tiles to accommodate the telephone/data/security cables installation.

Electrical contractor shall coordinate with the communication contractor to install conduits as required for the all systems and the 120V-24VDC transformer for electronic door lock devices at card reader locations as necessary.

Low voltage contractor shall furnish and install cable hangers with Caddy Clips in the attic, 4 hangers per 16 square feet, to support voice/data/ security cables as required by codes. All cables shall be installed prior to the installation of the ceiling grid if possible. The low voltage contractor shall be responsible for any damage, physical or cosmetic, to ceiling tiles. Electrical contractor shall be responsible to coordinate with cable contractor for the cable path requirement.

BUILDING SYSTEMS

3.2 SECURITY

3.2.1 INTRUSION DETECTION AND ALARM

A. System Description and Installation Requirement

The intent and purpose of this system shall be to provide a security/intrusion entry alarm system in the building. All perimeter doors, roof hatches, or other external entry points shall be equipped with dedicated, concealed magnetic contact switches. Interior protection shall be provided by combination passive infrared/microwave detectors and glass break sensors located as indicated on the drawings.

The alarm siren(s) shall be installed in the plenum above the keypad(s) as indicated on the drawings. Each alarm device shall report to the County Central Station as a **separate point**. Use point expander OctoPopit module(s) for the point expansion of the alarm panel and a separate enclosure(s) D8103 to house the expansion device(s). Install alarm cables **home run from each alarm device to the panel**. Appropriately sized "end of line" resistors shall be placed at the device end only. Installation of modules, devices and wiring shall be in accordance with Radionics design, engineering standards. Additional Power supplies, Batteries, OctoPopits, OctoRelays, and associated cables shall be mounted in additional D8103 cabinet(s). Maximum build out per D8103 or enclosure shall be 5 modules and or 2 7AH/12V batteries.

Installation of modules, devices and wiring shall be in accordance with current Radionics design, installation, and engineering standards. Additional D8132 Battery Charger / power supplies, batteries, OctoPopits, OctoRelays, and associated cables shall be mounted in additional D8103 cabinet(s). Maximum build out per D8103 or enclosure shall be 5 modules and or 2 each 7AH/12V batteries

The intrusion alarm cables shall be installed horizontally through the ceiling area in a neat and orderly fashion and supported by cable hangers at appropriate intervals. The cables shall be positioned at least six (6) inches from electrical equipment, electrical wiring, telephone cabling, intercom cabling and data wires. Exposed wiring shall only be permitted above ceiling level or ten feet from floor level. The installation shall comply with the County of Los Angeles Building Safety and Fire Codes. Contractor shall furnish, at his expense, all permits issued for scope of work. Contractor shall supply copies of all permits acquired.

The Radionics D7412/9412 Alarm Communicator Panel and associated equipment enclosures shall be installed in the MCR room. Clearance in front of all cabinets shall be a minimum of 36 inches. The alarm shall report to the County Central Station. Library Staff shall be responsible for obtaining an alarm permit from the local law enforcement authority.

The Radionics Alarm Communicator Panel shall power all peripheral alarm devices for 24 hours of standby time with 5 minutes in alarm condition conforming to NFPA 72 central station requirements in the event of power failure. Radionics load calculation worksheet page 61 & 63 of document 74-07692-000-D shall reflect all security equipment component current loads, standby battery requirements and standby battery calculations. Additional D8132 battery charger modules and batteries shall be installed in Radionics D8103 enclosures. All transformers shall be mounted in D8004 enclosures. The intrusion alarm equipment shall have a dedicated branch circuit identified and labeled with panel and branch circuit number on power receptacles covers.

Terminations and connections throughout system the shall employ terminal strips with rising wire clamp screws or solder terminals, all in cabinets or enclosures. Telephone punch type blocks, and electrical wire nuts are not acceptable. In cases where shielded cable is used, all shields will be grounded.

The alarm contractor shall be responsible for programming and testing the alarm panel in the local mode. The alarm contractor shall furnish the County with completed Radionics programming sheets and As-Built 8½" x 11" drawings(s) that indicate each device/point location identified to reflect 16 character idle text in programming on not less than 12 point text on floor plan. The alarm contractor shall submit as-built drawings as outlined in paragraph 1.05,D,1-5.

The alarm contractor shall be an authorized and current direct Radionics Dealer. The contractor must provide proof of dealership with Radionics. INC. as well as verification of prior experience with Radionics Controllers and System design, Detection Systems and have experience with programming system features. The installer must provide proof of training via a valid training certificate. Certificate must have been issued more than six (6) months and less than five (5) years prior to installation date. **Proof of dealership must be attached to this quotation.**

The alarm contractor shall be responsible for programming and testing the alarm panel in the local mode. The alarm contractor shall furnish the County with completed Radionics programming sheets and As-Built 8½" x 11" print(s) that indicate each device/point location identified to reflect unique and descriptive 16 character idle text in programming on not less than 12 point text on floor plan. The alarm contractor shall submit as-built drawings as outlined in paragraph 1.05,D,1-5.

The alarm contractor shall program the system to activate or arm at a time to be determined (see ISD Project Manager for coordination) each night except Saturdays, Sundays, and Holidays. The system will automatically disarm at 6:00A.M.. or by authorized staff or on-site security staff.

The alarm contractor shall provide hands on training to County staff in the operation of the system. A roster of attendees shall be documented..

If the intrusion alarm system is to be integrated with the access control system, the control panel will incorporate by means of programming and wiring logic, one or more input area disarming points and output area armed relays that will disarm the area(s) when armed, by means of a momentary contact closure received from the access control system. These areas may differentiate between perimeter and interior protective devices. Contact the Project's ISD Telecommunications Systems Engineer for details.

B. Materials and Equipment

a. Digital keypad – Radionics model D1255 Alpha IV.
b. Alarm panel – Radionics model D7412 or D9412, **RAM IV** or greater software.
c. Passive infrared / microwave detectors – Detection Systems DS970 (Long Range).
d. Passive infrared / microwave detectors – Detection Systems DS950 (Med. Range).
e. Passive infrared / microwave detectors – Detection Systems DS937 (360).
f. Glass break sensor – Sentrol 5810A.
g. Siren/Speaker – Sentrol MPI36.
h. Magnetic door contact switch, flush mount – Sentrol model 1078CT.
i. Magnetic door contact switch, surface mount, non-exposed wiring – Sentrol 1042TW
j. Magnetic door contact switch, surface mount, exposed wiring – Sentrol model 2505A.
k. Magnetic door contact switch, floor mount – Sentrol model 2707A.
l. Transformer enclosure – Radionics model D8004.
m. Non-fire enclosure – Radionics model D8103.
n. Battery – D126 two (2) required for fire panel.
o. Transformer – Radionics model D1640.
p. Keypad back boxes – Radionics model D56.
q. Aux relay – Radionics model D136.
r. Phone jack, modular – Radionics model D128.
s. Battery charger – Radionics D8132.
t. OctoPopit – Radionics 8128C.
u. OctoRelay – Radionics D8129.
v. Transformer kit – Radionics D8004.
w. Dual Phone line monitor – Radionics D928 (Fire alarm applications)
x. Alarm cable – plenum rated, stranded, PVC insulated. unshielded, 20 gauge or larger, 2 pair twisted wire for keypad, glass break sensors and passive infrared / microwave detectors. Plenum rated, stranded, PVC insulated, unshielded, 20 gauge or larger, 1 pair twisted wire for door switches.
y. Shielded wire shall be required if Radionics noise immunity design thresholds will be exceeded.
z. All other cables and hardware as required to make the system fully functional.

3.2.2 ACCESS CONTOL SYSTEM

A. System Description and Installation Requirement

The intent and purpose of this system shall be to provide Card Access Control, if required. The system design follows:

> The system design utilizes a Hirsch Velocity Software System design. There will be one server computer, as designated on the drawings. The software will allow for Library Staff to control access for only their doors and employees through the programming of the restricted database feature on the Access Control System Software. A second, remote computer may be required and installed as designated on the drawings. The system will provide the capability for remote access database management.
>
> If required, the system shall be integrated with the intrusion alarm system for after hours access to disarm areas independent of the other. This shall incorporate an access level output unique to a class of cardholders that when presented, will provide a dedicated momentary relay closure to disarm the intrusion alarm control system.

The General Contractor shall provide verification of prior experience with Hirsch / HID software based systems, and have experience with programming the restricted database feature.

The General Contractor shall furnish and install all proximity card readers as indicated on the drawings. The card readers shall be connected to locking devices on the doors at the locations specified on the drawings. To comply with ADA code requirements, all proximity card readers shall be installed within six (6) inches of the door they are controlling.

Each door shall have it's own dedicated, magnetic door contact switches at the card reader location which shall connect to the card access panel to reset the locking device at the door when opened.

The locking devices must be rated at 24Vdc. For Continuous Duty. Power supplies for the locking devices shall be mounted remotely in the nearest Telecommunications room (MCR, TR1.1, etc.).

Cabling shall incorporate wire gauge conductors that reflect less than a 10% voltage drop to any access control component.

The General contractor is to program system configuration and restricted database feature. There will be no equipment substitutions accepted in the Checkpoint entry system section. The Contractor shall provide fifty (50) initial cards with the system. The Contractor shall be responsible for initial programming of all requested time zones, access levels, card users and cards. The contractor shall be responsible to provide a minimum of four (4) hours user training on system use, programming, backing up critical database files and creating report templates.

The general contractor shall furnish and install the **Fail Secure** door locks. The purpose is to ensure that the door will stay latched in case of power failure. Panic hardware shall be provided on all Fail Secure doors for egress as specified on the drawings. Any penetrations of doors after UL Listing shall require UL re-certification.

Properly bond and ground all shields.

Provide UPS for ALL system components and equipment, including servers, workstations, monitors, enrollment stations, and accessories, for up to four (4) hours continuous use.

B. Materials and Equipment

a. Hirsch system to be determined.
b. Proximity reader – Universal wire – 5 wire conductor. HID
c. Proximity card – To Be determined.
d. Main Controller - To be determined
e. Terminal controller – Checkpoint AC-603.
f. Altronix SMP10-CTX Power Supplies
g. Altronix SMP3-CTX Power Supplies
h. UPS – APC Smart-UPS 1000VA USB & Serial XL 120V. Part Number: SUA1000XL.
i. 12Volt Backup Batteries for each panel, as required for four (4) hours
j. PC – **Minimum requirements** -- Intel Pentium IV 800 MHz, 512 MB memory, 20 gigabyte hard drive, 40X CD-ROM drive, CD-ROM-RW, floppy drive, US Robotic 56K modem, 15 inch monitor or better for both server and workstation. The operating system shall be Windows NT 4.0 with Service Pack 6 or greater.
k. Electrified Schlage Mortise Lock Bodies with hinge.
l. Von Duprin Panic Hardware Series #99 or #33 (as required) with electrified lever trim and Von Duprin electric power transfer unit #EPT-218.
m. Sentrol Door Contacts Style 1078CT
n. Magnetic door contact switch, flush mounted and closed loop.
o. Isolation Relays (For Elevator Control).
p. Cable – Magnetic door contact switch, plenum rated, stranded, shielded, 18 gauge minimum, 2-pair wire.
q. Cable – Card reader to terminal controller, plenum rated cable, 6 wire, 18 gauge minimum, stranded with overall shield.
r. Cable – Panic bar lock, plenum rated, stranded, 14 gauge minimum, 2 conductors with overall shield.
s. Cable – Electric strike, plenum rated, stranded 14 gauge minimum, 2 conductors with overall shield.
t. All other cables and hardware as required to make the system fully functional.
u. Fifty (50) cards for use with the system.

3.2.3 RESTROOM DOOR RELEASE

A. System Description and Installations Requirement

The intent of this system is to provide a door release from the Circulation Desk and the Children's Desk as required for the restroom door. It requires that a line of sight be established between the restrooms and the door release button. It may be incorporated with the Door Communications System in Section 3.2.4. It may also be integrated with the card access or intrusion alarm systems, Sections 3.2.1 and 3.2.2 respectively as required.

Contractor shall provide submittals for the system to include design and hardware required for making the system operational prior to ordering and installation for approval and sign-off by ISD Telecommunications Systems Engineer. The power supply shall be installed in the MCR. The door locking devices must be rated at 24-VDC for continuous duty.

It is the responsibility of the Contractor to coordinate with the general building contractor, electrician, or door contractor for installation schedule and to deliver a fully functional system.

B. Materials and Equipment

a. Power supply - 25Vdc, 3Amp with battery backup
b. Electric Strike – Von Duprin
c. Door button – Rutherford surface button
d. Cable – 18 guage, CMP twisted pair.

3.2.4 DOOR COMMUNICATIONS

A. System Description and Installations Requirement

The intent of this system is to provide communications for various doors throughout the facility. The doors requiring communications will be identified by the Library Capitol Projects Staff and ISD Telecommunications Systems Engineer. The staff entrance shall incorporate a two-way weather and tamper resistant phone that shall interface with the telephone system. The telephone system will be programmed to alert on selected phones when a call is made from the door phone. When a caller is authorized to enter, the receiver will select the appropriate code via the telephone keypad which will be passed to the door lock, releasing it for entry.

B. Materials and Equipment

a. Door Phone – Viking W-1000 or W-2000a
b. Door Entry Controllers - Viking C-1000, RC-2a. RC-3 (as required)
c. Flush Installation pre-wire box – Viking rough-in box P/N 259576
e. Surface/Vandal Resistant Mounting Box – Viking VE-5x5 Enclosure (as required)

3.3 PUBLIC ADDRESS SYSTEM

A. System Description and Installation Requirement

The intent of the system is to provide voice paging. The system will cover the entire library area. If zones are used, a maximum of three (3) zones will be assigned. The zones are 1) Staff, 2) Public, and 3) Emergency. The system will originate through the telephone system. Requirements shall include:

The paging equipment shall have 600 ohm balanced input for connection to the telephone system.

All speaker assemblies shall include a back box, grill and line matching transformer. The speakers shall include a built-in, screwdriver adjustable volume control and be equipped with a 25-volt line-matching transformer set on one (1) watt tap.

The paging system will allow for paging over the telephone instruments, overhead speakers, or both simultaneously.

The general paging equipment for the building shall be installed in the MCR and connected to the Norstar Meridian telephone system paging port using an RJ14-to-Spade terminating cable. It shall be mounted on the designated plywood backboard as indicated on the drawings. The communications contractor shall provide the telephone connection at an interface block.

The amplifier shall be sized appropriately to support all speakers.

The speaker cables shall be shielded twisted one (1) pair, 20 AWG, and CMP rated. The speaker cables shall be installed horizontally through the ceiling area in a neat and orderly fashion and supported by cable hangers at appropriate intervals. The speaker cables shall be positioned at least six (6) inches from telephone and data wires. The installation shall comply with ALL applicable Building Safety and Fire Codes.

B. Materials and Equipment

a. Amplifiers – Solid state, 100 watts RMS, 25/70-volt output, Bogen model TPU-100B.
b. Control modules – Bogen PCM-2000, Bogen ZPM-3, or Valcom V-2003A
c. Power supplies – Atlas/Soundolier model PS24 series or as required
d. Speaker – 8", 8 ohm, with 25/70 volt transformer and volume control, Quam model C5 VK or VS series.
e. Speaker enclosure – Quam model ERD 8 series.
f. Ceiling mounting bracket – Quam model SSB-2.
g. Open Truss Ceiling enclosure/mount – Atlas/Soundolier Model X8609
h. Optional suspension hanger for X8609 – Atlas/Soundolier 435 in appropriate length
i. Speaker cable – shielded twisted pair AWG #20, plenum (CMP) rated.

3.4 VIDEO

3.4.1 CCTV

A. System Description and Installation Requirement

The communication contractor shall install networked, color IP addressable, CCTV cameras where shown on the drawings. The image will be displayed using an "internet browser" on selected workstation PCs. A Digital Video recorder shall be installed at a location to be determined by the ISD Telecommunications Systems Engineer and Library Staff.

It is the responsibility of the communications contractor to coordinate with the general and electrical contractors for the installation schedule and to deliver a fully functional system.

B. Material and Equipment

a. Camera – Axis Network Video Camera 2120.
b. Power Supply – Altronix ALTV248
c. Viewing Software – Sharkseye Terrio LE
d. Digital Video Recorder – Pelco DX3000 Series
e. Video Receiver – NET101R-A | Single-channel video receiver with bi-directional audio and integrated Ethernet connection.
f. Video Transmitter – NET101T-A | Single-channel video transmitter with bi-directional audio and integrated Ethernet connection.
g. Cable – West Penn Plenecom
h. Cable – RG-6/U Type CATV/MATV Coaxial Cable Coaxial Cable 69. Gas injected foam polyethylene.
i. Cable – RG-59/U, plenum rated.
j. Connectors – as required. All faceplates shall be electrical Ivory
k. Tamperproof ceiling housing – Burle TC9366H.
l. Housing (outdoor) – PELCO EH 3512, w/wall mount EM1450.
m. Housing (indoor) – PELCO EH 3010, w/wall mount EM 1400.

3.4.2 MATV

3.4.3 SATV (Satellite)

3.4.4 CATV (Cable Access)

A. System Description and Installation Requirement

The intent of the system is to provide UHF/VHF/FM signals to the building. The system shall consist of a local cable TV company drop, internal coaxial cable, a distribution amplifier, and _____ (__) drops as indicated on the drawings. The communications vendor shall use pads as necessary to prevent overload of the signal.

B. Materials and Equipment
   a. Distribution Amplifier – Pico Macom, INC. TA-52, wall mounted (if necessary).
   b. Cable – West Penn Plenecom
   c. RG-6/U Type CATV/MATV Coaxial Cable Coaxial Cable 69. Gas injected foam polyethylene.

d. External cable P/N AQC841 Moisture Blocking (if required)
e. Internal cable P/N 25841
f. Connectors – as required. All faceplates shall be electrical Ivory

3.4.5 TELECONFERENCE SYSTEM

3.5 CABLING SYSTEM

3.5.1. Station Cable (Voice/Data)

a. The communications contractor shall be responsible for obtaining a low voltage installation permit from the appropriate authority before starting of installation.

b. The communications contractor shall be responsible for consulting with the building inspector to determine whether there are special local requirements for strapping the cables in the attic area.

c. The communications contractor shall be responsible for coordinating with the building's General Contractor to determine the cable routings, schedules for cable placement and ceiling inspection.

d. The communications contractor shall provide installation of the cable hangers and sleeves that will support the horizontal cables in the attic area per all applicable local building code(s).

e. The communications contractor shall furnish and install voice/data locations, voice only locations, and data only locations per approved floor plans.

f. The communications contractor shall furnish and install whips, wall plate adapters and floor plate adapters as shown on the drawings.

g. All voice/data outlets shall be furnished and installed complete with two (2) voice jacks (Cat 5e, RJ45) and two (2) data jacks (Cat 5e, RJ45) terminated with two (2) voice and two (2) data plenum rated cables unless otherwise noted on the drawings.

h. The data cables shall be either Berk-Tek LANmark-350 UTP or General Cable PlatinumPLUS Category 5e plenum rated 24 AWG four pair. The jacket shall be blue. Furnish and install two data cables at each jack location. All data cables shall be installed from the station jack directly to the appropriate Cat 5e patch panels in the MCR. All data cables shall be tested to minimum Cat 5e standards.

i. The voice cables shall be either Berk-Tek LANmark-350 UTP or General Cable Category 5e plenum rated 24 AWG four pair. The jacket shall be white. Furnish and install two voice cables at each jack location. The voice cables shall be installed from the station jack directly to the appropriate Cat 5e patch panel in the MCR. All pairs are to be terminated using TIA/EIA 568-A at both ends. All voice cables shall be tested to minimum Cat 5e standards.

j. The jack housings and faceplates shall have four (4) positions for jacks. Blank covers shall be installed in vacant jack positions. Jack housings and faceplates shall be compatible with the Mini-Jacks. The type and color is to be determined by the installed location. Some will be flush or non-flush. Modular furniture faceplates shall be color coordinated with the color of the furniture base plate. It will be the selected communications contractor's responsibility to furnish and install the proper jack housings and faceplates. The communications contractor shall determine the type of faceplate prior to the scheduled installation and must be approved by ISD Telecommunications Systems Engineer and Library Staff prior to use.

k. Floor monuments will be flush mount, single gang, and fully adjustable, with minimum of two (2) each one (1) inch conduit openings, unless otherwise noted on the plan. The Walker/Wiremold 880M1 Omnibox or 880W1shall be used unless otherwise noted on the plan. Where applicable, the Walker/Wiremold 817B flange, AC-MAB, 828GFI cover, AC-QP106 Quad telecommunications frame, and Walker/Wiremold 828R Brass Electrical Duplex Cover Plate, unless otherwise noted on the plan. Any deviation must receive written approval from the ISD Telecommunications System Engineer and Library Staff prior to use.

l. Floor monument mounting plates shall be Panduit CF-1064EI.

m. The communications contractor shall furnish and install patch panels and wire organizers. Separate patch panels shall be provided for the PUBLIC and STAFF areas. The patch panels shall be Panduit Mini-Com 48 port all metal modular, part number CP48BL. The wire organizers shall be Panduit WMPH-2. Furnish one (1) organizer per patch panel plus one (1) additional wire organizer at the top of each row of patch panels. Be sure to include the Mini-Jacks for the patch panel. Vertical wire minders shall also be furnished and installed as required using Panduit WMPV-C45 and Panduit WMPV-S45.

n. The RJ45 data jacks shall be wired according to TIA/EIA 568-A.

o. All jacks shall be modular Panduit Mini-Jacks. The voice jacks (Cat 5e, RJ45) shall be Mini-Jack part number EI5388EI (Electrical Ivory). The data jacks (Cat 5e, RJ45) shall be Mini-Jack part number CJ5E88OR (Orange) or CJ5E88BU (Blue) as shown on the plan.

p. The PUBLIC areas shall use Blue data jacks. The STAFF areas shall use Orange data jacks.

q. All voice/data jacks and patch panels shall be labeled according to Los Angeles County standard 802. Labels are to be typed or drawingsed with a labeling device and permanently affixed. No hand written lettering is acceptable. The labels shall be drawingsed on white tape with black lettering for jacks. Patch panels shall be labeled both front and back. The patch panel labels shall be black tape with white lettering, four (4) labels per strip. See the ISD Telecommunications Systems Engineer if further clarification is needed.

Sample Labeling: Voice – VYxxx (Voice cables are not split, but require separate

Data -- DYxxx cable for each, Y = Floor number, xxx = cable number beginning with 001.)

r. All wire and cable runs in the ceiling area shall be supported with ceiling hangers, supplied and installed by the selected communications contractor. Cables must be supported at a space interval that is allowable by code. At no point shall cable(s) rest on acoustic ceiling grids, panels or lighting support wires.

s. Cable shall be installed in continuous lengths (no splices allowed) from origin to MCR, using the **shortest route possible**, and shall be bundled in groups of not greater than 40 cables.

t. Four pair data cables shall be bundled with a Velcro type of tie, such as Panduit HLS, HLM, HLC or equivalent. Do not use plastic ties on data cables.

u. Furnish and install flexible tubing (Seal Tite) to conceal wire runs into modular furniture or where needed to secure multiple exposed cables.

v. It shall be the responsibility of the communications contractor to determine and furnish the quantity of voice/data wire needed.

3.5.2 Workstation Outlets

a. Unless otherwise noted on the drawing, each outlet location installed in the wall, on the modular furniture system and on the floor shall be equipped with two (2) Category 5e RJ45 type voice modular jacks, Electrical Ivory in color and two (2) Category 5e RJ45 type data modular jacks, Orange for the STAFF locations and Blue for the PUBLIC locations as shown on the plan.

b. Each outlet location shall be provided with two (2) voice cables and two (2) data cable. Unless otherwise indicated on the plan, voice cable pairs shall NOT be split between the two (2) jacks and shall be fully terminated.

c. Voice jacks in the field shall be Category 5e, 8 position, 8 wire with termination cap color, wired to the TIA/EIA 568-A wiring standard. Data jacks shall be Category 5e, 8 position, 8 wire with termination cap color, wired to the TIA/EIA 568-A wiring standard. Voice jacks as manufactured by Panduit (CJ5E88EI). Data jacks as manufactured by Panduit (CJ5E88OR or CJ5E88BU) as shown on the plan.

d. Panduit (CFPE4) shall mount jacks on a four- (4) module, Electircal Ivory, faceplate for the wall.

e. Where outlet location is specified for a wall-mounted telephone, provide and install a voice cable terminated on a RJ25 jack with a single module faceplate by Panduit (CJ641EI).

f. Provide and install appropriate faceplate, extender as determined by modular furniture brand. The communications contractor shall determine bracket type and color prior to scheduled installation.

g. If faceplates are mounted to double gang boxes, the communications contractor shall provide and install, as required, In-Wall box adapters as manufactured by Panduit.

h. The communications contractor shall be responsible to install cover plates or blank modules of the appropriate color on any unused single or double gang boxes. Modules by Panduit (CMB).

i. Data jacks shall occupy the bottom positions on the faceplate. Data jacks in horizontally oriented faceplates shall occupy the right-most positions.

j. The communications contractor shall provide cross-connect jumpers as required from the MPOE to MCR, between MCR's and IDF's and for faxes, modems, elevator phones, etc. as required.

k. Any deviation/substitution must be verified and approved in writing by the ISD Telecommunications Systems Engineer prior to use.

3.5. DISTRIBUTION CABLE (where applicable)

3.5.1. Voice Cable

a. The communications contractor shall provide, install and terminate an appropriately sized, as determined by the ISD Telecommunications Systems Engineer and Library Staff, CMR rated cable to provide connectivity between the MPOE and MCR.

b. Backbone cables shall be installed separately from the station cables. Where both cables are installed in a cable tray or wire way, backbone cables shall be installed first and bundled separately from the station cables.

3.5.2. Fiber Optic Cable

1. If required, fiber optic cable shall be jacketed as appropriate for use in an underground environment.

2. The cable shall be composite, tight buffered, all dielectric, Kevlar strength members with polyethylene outer jacket (medium or high density) with 600 lbs pull-strength. Individual fibers shall be covered with a 900-micron primary buffer. The cable shall contain continuous glass with Corning or Lucent Technologies glass only, and no splices.

3. The cable shall consist of 8 Multi-mode fibers and 4 Single-mode fibers and shall meet or exceed the following specifications.

   a. Multi-mode: diameter (microns) 62.5/125; dual window (850/1300): maximum attenuation @ 850/1300 nm < 3.15/1.5 db/Km: minimum bandwidth (MHz-km) @ 850/1300 nm, 160/500: graded index.

   b. Single-mode: diameter (microns) 8.3/125: dual window (1310/1550) maximum attenuation @ 110/1550 nm, < 4.3 db/km.

c. The communications contractor shall ensure that the multi-mode fiber optic cables can support FDDI, 100Base-FX, and 1000Base-FX protocols, and the single-mode fiber optic cables can support 1000Base-LX and 1000Base-SX protocols.

d. The communications contractor shall furnish and install a rack mounted 12-port fiber distribution enclosure by Siecor or equivalent, fully equipped with couplers in the MCR.

Note: The Fiber Patch Panel Assemblies shall be mounted above the core chassis' on the relay racks.

e. The communications contractor shall furnish, install and terminate all fiber optic strands on ceramic type of ferrule connectors in each distribution enclosure, install SC type of connectors for the multi-mode cables and FC/PC (Physical Contact) for the single-mode cables.

f. The communications contractor shall also furnish and install one-inch diameter inter-duct for fiber runs.

g. The communications contractor shall furnish and install each span of the fiber optic cables in one continuous length, no splices, utilizing building conduits and sleeves.

h. The communications contractor shall provide hardware for termination and cable securing, such as clamps, tie-raps, soft buffer, spiral wrap or split loom, SC connectors, etc.

i. The communications contractor shall leave at least ten (10) feet of fiber optic cables slack on top of cable tray.

j. The communications contractor shall provide other services, if required, to complete, such as: tighten barrel connectors, secure cable to fiber distribution panel, and install connectors to couplers, place fiber distribution enclosures in rack.

3.6 CABLE TESTING

3.6.1. General

a. All testing shall be per the Los Angeles County STD-902 Testing Standard. An orientation with the ISD Telecommunications Systems Engineer and Library Staff shall take place on site prior to the test. It shall be scheduled at least one week in advance. The ISD Telecommunications Systems Engineer and/or Library Staff shall certify prior to testing the following:

b. Test meters have been calibrated to TIA/EIA Standard within the last 12 months. With a Certificate of Compliance, meter serial number and dated.

c. Test meter shall be fully charged.

d. Test configuration set to the County Standards.

e. Manufacturers warranty certification (if applicable) requirements shall be reviewed to ensure that all warranty requirements are met.

f. The communications contractor shall furnish three (3) drawingsed copies and one copy on CD-ROM, with the complete set of test results. Copies of PC based software to view drawings and results shall also be provided to the ISD Telecommunications Systems Engineer and appropriate Library Staff.

3.6.2 Communications Contractor Requirements

a. Communications Contractor shall provide sufficient skilled labor to complete testing within the agreed upon test period. Testing shall commence no later than _____ and be completed no later than _____.

b. Communications Contractor company shall have a minimum of 3 years experience installing and testing structured cabling systems. All installers assigned by the Contractor to the installation shall have factory certification that they are qualified to install and test the provided products.

c. Communications Contractor is responsible for supplying all of the required test equipment used to conduct acceptance tests.

d. Communications Contractor is responsible for submitting acceptance documentation as defined in section 3.6.5 below.

3.6.3 Test Process

d. The County reserves the right to be present during any or all of testing.

e. Testing shall be of the Permanent Link. However, the communications contractor shall warrant performance (see Part 3) based on Channel performance and provide patch cords that meet channel performance.

f. All cabling not tested strictly in accordance with these procedures shall be re-tested at no additional cost to the County.

g. 100% of the installed voice and data cabling must be tested. All tests must pass acceptance criteria defined in 3.6.5.d.

h. Test equipment shall be fully charged prior to each days testing.

3.6.4 Standards Compliance & Test Requirements

a. Cabling must meet the indicated performance specifications:

_____ TIA 568B Category 5e

_____ TIA 568A Category 6 Addendum (draft 5 or latest)

b. All test equipment used must meet the performance specifications defined in section 3.6.6. below.

3.6.5. Documentation

a. Test reports must be submitted in hardcopy and electronic format. Hand-written test reports are not acceptable.

b. Hardcopy reports are to be submitted in labeled 3 ring binders with an attached affidavit verifying passing execution of all tests. For large installations electronic reports with hardcopy summaries are preferred. Hardcopy summary reports shall contain the following information on each row of the report: circuit ID, test specification used, length, date of test, and pass/fail result.

c. Electronic reports are to be submitted on CD-ROM only. If proprietary software is required to view test results, the software shall be provided to ISD Telecommunications Systems Engineer and appropriated Library Staff. If the results are delivered in a standard format like Excel, Access, CSV files, etc. then software to read these files need not be provided. Electronic reports must be accompanied by a Certificate signed by an authorized representative of the Contractor warranting the truth and accuracy of the electronic report. Certificate must reference traceable circuit numbers that match the electronic record.

d. Test reports shall include the following information for each cabling element tested:

i. Wiremap results that indicate the cabling has no shorts, opens, miswires, split, reversed, or crossed pairs, and end to end connectivity is achieved.

ii. For Category 5e or 6 cabling: Attenuation, NEXT, PSNEXT, Return Loss, ELFEXT, and PSELFEXT data that indicate the worst case result, the frequency at which it occurs, the limit at that point, and the margin. These tests shall be performed in a swept frequency manner from 1 MHz to highest relevant frequency, using a swept frequency interval that is consistent with TIA and ISO requirements. Information shall be provided for all pairs or pair combinations and in both directions when required by the appropriate standards. Any individual test that fails the relevant performance specification shall be marked as a FAIL.

iii. Length (in meters), propagation delay, and delay skew relative to the relevant limit. Any individual test that fails the relevant performance specification shall be marked as a FAIL.

iv. Cable manufacturer, cable model number/type, and NVP

v. Tester manufacturer, model, serial number, hardware version, and software version

vi. Circuit ID number and project name

vii. Autotest specification used

viii. Overall pass/fail indication

ix. Date of test

x. Test reports shall be submitted within 7 business days of completion of testing.

3.7.6 Test Equipment

a. Test equipment used under this contract shall be from manufacturers that have a minimum of 5 years experience in producing field test equipment. Manufacturers must be ISO 9001 certified.

b. All test tools of a given type shall be from the same manufacturer, and have compatible electronic results output.

c. Test adapter cables must be approved by the manufacturer of the test equipment. Adapters from other sources are not acceptable.

d. Baseline accuracy of the test equipment must exceed TIA Level III, as indicated by independent laboratory testing.

e. Test equipment must be capable of certifying Category 5e and 6 links.

f. Test equipment must be capable of storing full frequency sweep data for all tests and drawingsing color graphical reports for all swept measurements.

g. Test equipment must include S-Band time domain diagnostics for NEXT and return loss (TDNXT and TDRL) for accurate and efficient troubleshooting.

h. Test equipment must be capable of running individual NEXT, return loss, etc measurements in addition to autotests. Individual tests increase productivity when diagnosing faults.

i. Test equipment must include a library of cable types, sorted by major manufacturer.

j. Test equipment must store Category 5e or 6 autotests in internal memory.

k. Test equipment must be able to internally group autotests and cables in project folders for good records management.

l. Test equipment must include DSP technology for support of advanced measurements.

m. Test equipment must make swept frequency measurements in compliance with TIA standards.

n. The measurement reference plane of the test equipment shall start immediately at the output of the test equipment interface connector. There shall not be a time domain dead zone of any distance that excludes any part of the link from the measurement.

3.7.7. Fiber

a. The communications contractor shall perform end-to-end fiber optic strand testing per Los Angeles County Fiber Testing Standard with the following minimum quality levels: Optical Time Domain Reflectometer (OTDR) with drawingsout (both directions) and absolute dB loss (power meter), at 850 nanometers for multi-mode and 1310 nanometers for single-mode. All fiber optic cable lengths less than 600 feet shall require a certified kilometer to be used with the OTDR testing equipment. After testing on the reel has been successfully completed, fiber optic system shall be installed with all patch cords attached and then the entire channel shall be tested.

b. The communications contractor shall perform two sets of OTDR drawingsouts with the above mentioned minimum quality levels. The first OTDR reading and drawingsout must be done on-site and submitted to the Project Manager prior to the utilization of the fiber, and the second OTDR reading and drawingsout must be done after installation.

c. Upon completion of the fiber optic portion of this project, the communications contractor shall provide two complete sets of OTDR traces on 8 ½ x 11" sheets. The communications contractor shall annotate on each OTDR trace 1) direction of test per strand (from-to); 2) bundle number; 3) buffer color and 4) strand color. Communications contractor-provided representations of the test data are not acceptable.

3.8 VOICE/COMMUNICATIONS SYSTEMS

3.8.1. System Description and Installation Requirements

f. The communications contractor shall furnish, install, and make operational a complete Norstar-PLUS Modular ICS telephone system Analog Trunk configuration, wired and equipped with _____ trunks and _____ stations and all associated equipment to make the system operational The telephone system shall be installed in the MCR as indicated on the drawings.

g. The communications contractor shall furnish and install a total of _____ (__) model M7208 instruments. The communications contractor shall furnish and install _____ (__) model T7316 instruments as noted on drawings for the new facility. The communications contractor shall furnish and install _____ (__) model M7406 (Black only) Cordless instruments as noted on drawings for the new facility. All telephones shall be color ash or gray as determined by Library Staff.

h. Library Staff shall provide the communications contractor with all the information required to develop the user database (i.e., key sheets, numbering plan, class of service, number of analog and digital phones, etc.). The information shall be forwarded to the communications contractor six (6) weeks prior to the scheduled cut-over date. Change requests submitted in the (six week) interim will be held until after cutover and then processed as a change order on a time and material basis.

i. One week after the telephone system is in full operation the communications contractor and ISD Telecommunications Systems Engineer and Library Staff will test all newly installed equipment. A Certificate of Acceptance will be signed by the ISD Telecommunications Systems Engineer and Library Staff. The warranty of the telephone system will start on the signature date.

j. The communications contractor shall cross-connect fax and modem lines and trunks as required and determined by ISD Telecommunications Systems Engineer and Library Staff. Trunks and locations for faxes and modems to be determined during installation.

k. The communications contractor shall provide paging port connection to paging amplifier using an RJ14-to-Spade terminating cable.

l. The communications contractor shall provide two (2) RJ45 jacks adjacent to alarm panel for dial tone for the alarm system. The lines to be used will be ordered by County Library Staff. The communications contractor will terminate the lines on the blocks. The alarm contractor will terminate the lines into the alarm.

m. The communications contractor shall provide and install in the relay rack a 110-type

termination Cat5e patch panel, Panduit P/N DP485E88110U for voice patching capabilities. The voice cables from the telephone system shall be terminated on this panel.

n. The telephone system shall be equipped with Startalk Auto-Attendant and voice mail to support the number of users and lines. The Library Staff will be responsible for sizing the system.

3.9 MEETING ROOM

3.10 EQUIPMENT RACKS / MOUNTINGS

a. The contractor shall provide and install equipment racks that are earthquake rated for zone 4 and shall be securely installed according to Los Angeles County Standard 108. This standard will require the use of a 3-inch spacer bar P/N STD108DET4).

b. The contractor shall provide and install standard 7' by 19" aluminum relay rack(s) (Chatsworth P/N 48353-703, color Black, shelves and cable trays as specified in the attached drawing. The contractor shall install, position, reposition, or remove racks and equipment as required without disruption of ongoing services. The contractor shall furnish extension cables, power taps, or temporary racks if needed.

c. All equipment racks shall be augmented with horizontal and vertical management hardware, both front and rear, to properly dress cables and patch cords. Wire management hardware by Panduit (WMBVC).

d. The number of equipment racks shall be determined by ISD Telecommunications Engineer and Library Staff. The number shall be dependent on the size of the Library.

e. All voice/data cables shall be terminated on separate patch panels in the MCR. Patch panels shall be dedicated to voice, STAFF data, and PUBLIC data. See section 3.4 for requirements. The cables shall be terminated and label sequentially on the patch panels.

f. Cable trays shall be Chatsworth Products, INC. (CPI) P/N 11252-713. Color, black.

g. All structural ironwork shall be UL-certified, providing the best bonding for static and grounding. Painted structural ironwork is not allowed.

h. Cable tray shall be of the tubular type construction. The tray shall be installed with the rungs on the topside of the tray. All attachments to drywall shall be on ¾" plywood.

i. Cable tray shall be 7'3" from the finish floor. This will require the installation of a 3" (Black) spacer manufactured by B-Line Systems, INC., P/N STD108DET4. The 7'3" allows for the cable tray to be positioned over the 7' doorway.

j. Structural cable tray, relay racks, cabinets, systems, attachments and earthquake bracing shall comply with Zone 4 earthquake, NEMA, NEC and TIA/EIA-569 standards. Floor mounting hardware shall be a 3/8" bolt, lock washer, flat washer, with anchor in the floor, quantity as required.

k. All exposed cut and sharp edges shall be deburred and filed to a safe finish. Cable tray runway ends shall be capped with a black rubber cap.

l. Relay racks shall be high strength aluminum construction with universal 5/8"-5/8"-1/2" tapped mounting hole #12-24 thread pattern on both front and rear. Designed and seismic built to the EIA-310C Standard.

m. All equipment racks shall be augmented with horizontal and vertical management hardware, both front and rear, to properly dress cables and patch cords. Wire management hardware shall be by Panduit.

n. The communications contractor shall install, position, reposition, or remove racks and equipment as required without disruption of ongoing services. The communications contractor shall furnish extension cables, power taps, or temporary racks if needed.

PART 4 EXECUTION

4.1 INSTALLATION

A. General

All equipment shall be installed in accordance with the published practices of the equipment manufacturer, applicable FCC regulations, generally accepted industry standards, cited codes and standards, and these specifications.

B. Temporary Installation

The contractor shall temporarily install all electronic equipment for the final tests of the equipment and the systems, and then shall remove and store all equipment which is not built-in until occupancy by County personnel. The contractor shall then return and make complete and final installation and check-out.

C. Equipment Not Installed

Equipment not meant for installation and all spares shall be delivered on site, to Library Capital Projects Staff and secured.

D. Wiring

Terminations and connections throughout all systems shall employ one of the following methods:

1. Solder terminals, telephone-type punch terminal strips or machine wire-wrapped terminals in all cabinets.

2. Crimp connectors at outlet boxes and screw type or plug and socket connections at all equipment. Note that crimp-type connections are approved only for stranded wire.

3. 66-Type blocks shall only be used for voice distribution cables. They are not permitted for any other installation.

E. Labels

All controls, function switches, etc. shall be clearly labeled on all equipment panels. This labeling shall be permanently etched or engraved. Neat nameplates engraved on two-layer plastic and affixed with epoxy glue may be used.

F. Flexible Wire

Stranded wire and flexible cable shall be used for all connections to equipment not permanently attached to walls, floors or racks.

G. Conduits

1. Thin wall conduit shall be used for conduits 2" in diameter or less. For conduits over 2" in diameter, rigid steel galvanized shall be used. However, if it is necessary to use flex duct or plastic PVC, prior approval must be obtained in writing from ISD Telecommunications Systems Engineer and the next larger size flex duct or PVC shall be used. The flex shall be anchored at all bends and runs between bends must be straight and non-zigzagging through studding, joints, etc. If PVC conduit is to be used, use steel galvanized conduit for all bends over 15 degrees.

2. All communications conduit shall be one (1) inch inside diameter unless otherwise noted on the drawings.

3. A 1/4 inch nylon pull line shall be installed in each conduit. For conduits over two (2) inch in diameter, provide three-eighth (3/8) inch nylon pull line.

4. All conduits shall be clearly and permanently identified at all terminals or cabinets as to its terminating end.

5. Individual communications conduit runs shall not have more than the equivalent of two (2) 90-degree bends, the ISD Telecommunications Systems Engineer shall be contacted to determine the size, type and location of a pull box that must be installed. Pull boxes shall not be used for transitions in conduit runs.

6. The radius of any conduit bend shall not be less than ten (10) times the inside diameter of the conduit. Except conduit for fiber optic cable. The conduit-bending radius shall have a miminum of 20 times of the O.D. of the install fiber optic cable.

7. Open ends of conduit shall be plugged during construction to prevent the entrance of moisture or foreign material. If moisture or foreign material is found at the time telephone and data cables are being installed, it shall be the responsibility of the contractor to thoroughly clean the conduit before the cable installation proceeds.

8. All conduits shall be securely fastened in place and shall be free from burrs, defects or obstructions that could interfere with the installation of cables.

9. All conduit, unless otherwise noted on drawingss, shall terminate on designated communications backboards either three (3) inches above the floor or six (6) inches below the ceiling.

10. All conduits shall be reamed and secured by locknut where applicable. All conduits shall have bushings on both ends.

11. All conduit not terminating in terminals, cabinets or outlet boxes shall be capped.

12. Conduit and fittings shall be homogeneous throughout and free from visible cracks, holes, foreign objects or other defects.

13. Empty conduit/sleeves, unless noted otherwise, shall be run to and between respective communications rooms and/or closets, as shown on the plans.

14. All underground communications conduit shall be PVC and shall have a minimum earth cover of eighteen (18) inches, except where subject to vehicular traffic (including road right-of-way) the PVC conduit shall be concrete encased with a minimum of thirty (30) inches of earth cover. Telephone conduit may be buried in the same trench as power (480 Volts or less) if separated by a minimum of three (3) inches of concrete or twelve (12) inches of dirt.

15. The number of outlets included in each home run shall be specifically limited, as shown on the plans, and shall not be exceeded.

16. The ISD Telecommunications Systems Engineer is responsible for duct assignments and shall be contacted before the installation of cables in the conduits.

17. Any deviation/substitution must be verified and approved in writing by the ISD Telecommunications Systems Engineer prior to use.

H. Outlets

All communications outlets shall be installed at the same height above the finished floor, unless otherwise noted on the drawingss, as the electrical outlets, and shall be:

1. For single conduit entrance, 4 11/16 inches x 2 1/8 inches x 2 1/8 inches.

2. For two (2) or more conduit entrances, 4 11/16 inches x 4 11/16 inches x 2 1/8 inches.

3. Plaster rings are required. Tiger Box rings may not be used.

4. All core-drilled holes in counter tops shall be three (3) inches in diameter. A removable/reusable grommet and cover shall be installed.

4.2 ACCEPTANCE AND TEST INSPECTION

A. Final tests and inspection shall be conducted after the contractor has submitted the Final Submittal. The final acceptance tests and inspection shall demonstrate the proper operation of each systems and its compliance with the drawings and specifications.

B. Written procedures for the tests not included above shall be prepared by the contractor and submitted for review and approval by the ISD Telecommunications Systems Engineer and Library Staff at least 30 days prior to the test. The contractor shall supply personnel and, wherever required, auxiliary equipment for the test, without cost to the County.

C. The County reserves the right to conduct, using contractor equipment and labor, a random re-test of up to five (5) percent of the cable plant to confirm documented results. Random re-testing, if performed, shall be at the expense of the contractor, using standard labor rates. Any failing cabling shall be re-tested and restored to a passing condition. In the event more than two (2) percent of the cable plant fails during re-test, the entire cable plant shall be re-tested and restored to a passing condition at no additional cost to the County.

4.3 TRAINING

A. The contractor shall conduct training on each product in PART 2, except that the County may waive training on any products with which the County technicians and operators are already trained or for which training is inappropriate. The contractor shall furnish the services of a competent instructor for classroom and hands-on instruction in the operation and maintenance of the equipment supplied. The training shall be sufficient to qualify County technicians to maintain the equipment and systems.

B. All training, plans, and materials shall be submitted by the contractor for review and approval by the ISD Telecommunications Systems Engineer at least 30 days prior to acceptance tests.

C. Classroom space for training will be provided by the County. All training classes shall be conducted on a mutually agreeable schedule prior to system acceptance.

D. Operator training curriculum, if required, shall be comprehensive enough to enable County personnel receiving initial training to independently conduct training classes and instruct other operators. The contractor shall conduct training and furnish training materials for up to 20 students, as determined by County.

E. Maintenance training. The communications contractor, if required, shall include in his maintenance training plan the recommended duration of maintenance training necessary to thoroughly cover the subject matter. This plan is subject to revision based upon County review.

F. The contractor shall furnish training materials to each student, which they shall keep. The training material shall include the Systems Manual, less appendices. Maintenance training shall be conducted twice to provide training for up to 10 students in each session.

G. The contractor shall provide one formal, technical training seat for each product installed.